TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Destinataire:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année) 02 août 1999 (02.08.99)	
Demande internationale no PCT/FR98/02348	**Référence du dossier du déposant ou du mandataire**
Date du dépôt international (jour/mois/année) 03 novembre 1998 (03.11.98)	**Date de priorité** (jour/mois/année) 04 novembre 1997 (04.11.97)
Déposant KREMER, Gilles etc	

1. L'office désigné est avisé de son élection qui a été faite:

[X] dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

03 juin 1999 (03.06.99)

[ ] dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection [X] a été faite

[ ] n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé
Antonia Muller

no de téléphone: (41-22) 338.83.38

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 98/02348

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9600485 A	04-01-1996	US 5668876 A	16-09-1997
		AU 692881 B	18-06-1998
		AU 2688795 A	19-01-1996
		CA 2193819 A	04-01-1996
		EP 0766902 A	09-04-1997
		FI 965161 A	13-02-1997
		JP 10502195 T	24-02-1998
GB 2328310 A	17-02-1999	NONE	
NL 1007409 C	18-11-1997	NONE	
EP 0745961 A	04-12-1996	US 5708422 A	13-01-1998
		CA 2176163 A	01-12-1996
		JP 8339407 A	24-12-1996
EP 0416482 A	13-03-1991	JP 3179863 A	05-08-1991
		DE 69023843 D	11-01-1996
		DE 69023843 T	13-06-1996
		US 5315634 A	24-05-1991
US 5479510 A	26-12-1995	NONE	
WO 9519593 A	20-07-1995	AU 1390395 A	01-08-1995
		GB 2300288 A	30-10-1996
US 5371797 A	06-12-1994	NONE	
EP 0565279 A	13-10-1993	AT 153159 T	15-05-1997
		AU 3533093 A	07-10-1993
		CA 2087886 A,C	07-10-1993
		DE 69310604 D	19-06-1997
		DE 69310604 T	04-09-1997
		ES 2101227 T	01-07-1997
		HK 1002716 A	11-09-1998
		JP 6046162 A	18-02-1994
		US 5406619 A	11-04-1995
WO 9530975 A	16-11-1995	FR 2719730 A	10-11-1995
		EP 0710386 A	08-05-1996
		JP 8512419 T	24-12-1996
		US 5740232 A	14-04-1998
WO 9412954 A	09-06-1994	US 5539189 A	23-07-1996
		AU 5556694 A	22-06-1994

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 98/02348

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F H04Q G06F

Documentation consultée autre que la documentation minimale dans la mesure ou ces documents relèvent des domaines sur lesquels a porte la recherche

Base de donnees electronique consultee au cours de la recherche internationale (nom de la base de donnees, et si realisable, termes de recherche utilises)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégone °	Identification des documents cites, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 96 00485 A (ERICSSON TELEFON AB L M) 4 janvier 1996 voir le document en entier ---	1-4, 25-29
E	GB 2 328 310 A (TSE HO KEUNG) 17 février 1999 voir le document en entier ---	1-29
P,X	NL 1 007 409 C (NEDERLAND PTT) 18 novembre 1997 voir le document en entier ---	1-4,29
A	EP 0 745 961 A (AT & T CORP) 4 décembre 1996 voir colonne 5, ligne 15 - colonne 16, ligne 31; revendications 1-35; figures 1,7-14 --- -/--	1-29

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiques en annexe

° Categones speciales de documents cités:

"A" document définissant l'etat general de la technique, non considéré comme particulièrement pertinent

"E" document anterieur, mais publié à la date de dépôt international ou apres cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cite pour determiner la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se referant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais posterieurement à la date de priorite revendiquée

"T" document ultérieur publié après la date de depôt international ou la date de priorite et n'appartenenant pas à l'etat de la technique pertinent, mais cité pour comprendre le principe ou la theorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être consideree comme nouvelle ou comme impliquant une activité inventive par rapport au document considere isolement

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activite inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison etant evidente pour une personne du metier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevee	Date d'expedition du present rapport de recherche internationale
23 avril 1999	04/05/1999

Nom et adresse postale de l'administration chargee de la recherche internationale	Fonctionnaire autorise
Office Europeen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

Formulaire PCT/ISA/210 (deuxieme feuille) (juillet 1992)

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

[redacted] internationale No
PCT/FR 98/02348

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 9600485	A	04-01-1996	US	5668876 A	16-09-1997
			AU	692881 B	18-06-1998
			AU	2688795 A	19-01-1996
			CA	2193819 A	04-01-1996
			EP	0766902 A	09-04-1997
			FI	965161 A	13-02-1997
			JP	10502195 T	24-02-1998
GB 2328310	A	17-02-1999	AUCUN		
NL 1007409	C	18-11-1997	AUCUN		
EP 0745961	A	04-12-1996	US	5708422 A	13-01-1998
			CA	2176163 A	01-12-1996
			JP	8339407 A	24-12-1996
EP 0416482	A	13-03-1991	JP	3179863 A	05-08-1991
			DE	69023843 D	11-01-1996
			DE	69023843 T	13-06-1996
			US	5315634 A	24-05-1991
US 5479510	A	26-12-1995	AUCUN		
WO 9519593	A	20-07-1995	AU	1390395 A	01-08-1995
			GB	2300288 A	30-10-1996
US 5371797	A	06-12-1994	AUCUN		
EP 0565279	A	13-10-1993	AT	153159 T	15-05-1997
			AU	3533093 A	07-10-1993
			CA	2087886 A,C	07-10-1993
			DE	69310604 D	19-06-1997
			DE	69310604 T	04-09-1997
			ES	2101227 T	01-07-1997
			HK	1002716 A	11-09-1998
			JP	6046162 A	18-02-1994
			US	5406619 A	11-04-1995
WO 9530975	A	16-11-1995	FR	2719730 A	10-11-1995
			EP	0710386 A	08-05-1996
			JP	8512419 T	24-12-1996
			US	5740232 A	14-04-1998
WO 9412954	A	09-06-1994	US	5539189 A	23-07-1996
			AU	5556694 A	22-06-1994

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire	**POUR SUITE A DONNER** voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après	
Demande internationale n° PCT/FR 98/ 02348	Date du dépôt international *(jour/mois/année)* 03/11/1998	(Date de priorité (la plus ancienne) *(jour/mois/année)* 04/11/1997
Déposant KREMER, Gilles et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

[X] Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. **Base du rapport**

a. En ce qui concerne la **langue,** la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.

[ ] la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.

b. En ce qui concerne **les séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :

[ ] contenu dans la demande internationale, sous forme écrite.

[ ] déposée avec la demande internationale, sous forme déchiffrable par ordinateur.

[ ] remis ultérieurement à l'administration, sous forme écrite.

[ ] remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.

[ ] La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.

[ ] La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. [ ] **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. [ ] **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre,**

[X] le texte est approuvé tel qu'il a été remis par le déposant.

[ ] Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne **l'abrégé,**

[X] le texte est approuvé tel qu'il a été remis par le déposant

[ ] le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n° 2

[ ] suggérée par le déposant.

[X] parce que le déposant n'a pas suggéré de figure.

[ ] parce que cette figure caractérise mieux l'invention.

[ ] Aucune des figures n'est à publier.

RAPPORT DE RECHERCHE INTERNATIONALE

Demande Internationale No
[redacted]/FR 98/02348

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 6 G07F H04Q G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 96 00485 A (ERICSSON TELEFON AB L M) 4 janvier 1996 voir le document en entier ---	1-4, 25-29
E	GB 2 328 310 A (TSE HO KEUNG) 17 février 1999 voir le document en entier ---	1-29
P,X	NL 1 007 409 C (NEDERLAND PTT) 18 novembre 1997 voir le document en entier ---	1-4,29
A	EP 0 745 961 A (AT & T CORP) 4 décembre 1996 voir colonne 5, ligne 15 - colonne 16, ligne 31; revendications 1-35; figures 1,7-14 --- -/--	1-29

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'inven tion revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
23 avril 1999	04/05/1999

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

1

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
A	EP 0 416 482 A (HITACHI LTD) 13 mars 1991 voir le document en entier	1-11, 14-16, 28,29
A	US 5 479 510 A (OLSEN KURT B ET AL) 26 décembre 1995 voir le document en entier	1-5,8, 11,14, 16,28,29
A	WO 95 19593 A (KEW MICHAEL JEREMY ;LOVE JAMES SIMON (GB)) 20 juillet 1995 voir le document en entier	1-4, 25-29
A	US 5 371 797 A (BOCINSKY JR RONALD V) 6 décembre 1994 voir abrégé; revendications 1-9; figures 1-4	1-4, 6-14,16, 28,29
A	EP 0 565 279 A (AMERICAN TELEPHONE & TELEGRAPH) 13 octobre 1993 voir abrégé; figures	1
A	WO 95 30975 A (FRANCE TELECOM ;POSTE (FR); COGECOM (FR); PAILLES JEAN CLAUDE (FR)) 16 novembre 1995 voir page 6, ligne 11 - page 12, ligne 20	1
A	WO 94 12954 A (WILSON SHEILA) 9 juin 1994	

1

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference ./.	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR98/02348	International filing date (*day/month/year*) 03 November 1998 (03.11.98)	Priority date (*day/month/year*) 04 November 1997 (04.11.97)
International Patent Classification (IPC) or national classification and IPC G07F 7/10		
Applicant KREMER, Gilles		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 3 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
03 June 1999 (03.06.99)	14 February 2000 (14.02.2000)
Name and mailing address of the IPEA/EP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR98/02348

I. Basis of the report

1. This report has been drawn on the basis of (*Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

☐ the international application as originally filed.

☒ the description, pages 1-47, as originally filed,
pages _____, filed with the demand,
pages _____, filed with the letter of _____,
pages _____, filed with the letter of _____.

☒ the claims, Nos. _____, as originally filed,
Nos. _____, as amended under Article 19,
Nos. _____, filed with the demand,
Nos. 1-10, filed with the letter of 02 February 2000 (02.02.2000),
Nos. _____, filed with the letter of _____.

☒ the drawings, sheets/fig 1/13-13/13, as originally filed,
sheets/fig _____, filed with the demand,
sheets/fig _____, filed with the letter of _____,
sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

☐ the description, pages _____

☒ the claims, Nos. 11-29

☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

See separate sheet.

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

4. Original statement of the amended claims

1. The method according to the amended Claim 1 is based on the embodiments described in connection with Figures 4 to 8.

The device according to Claim 9 implements the claimed method and does not extend the technical teaching of the application as filed.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-10	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-10	NO
Industrial applicability (IA)	Claims	1-10	YES
	Claims		NO

2. Citations and explanations

2. WO-A-96/00485 (D1) describes a message transmission method wherein a user (Figure 1: personal unit 20, terminal 22) makes contact with an information processing system (service node 26, in combination with an authentication centre 30 - see page 5, lines 14 to 26).

Before providing the desired service (home banking, D1, page 12, line 21 to page 13, line 20; recording telephone calls, D1, page 13, line 21 to page 14, line 3), the information processing system executes an authentication routine (D1, page 9, line 1 to page 12, line 20) during which the information processing system:

- sends a unique code (page 7, line 32) to the user (20, 22) on a first transmission medium (authentication challenge network 28), and
- receives the unique code from the user on a second transmission medium (service access network 24).

If the code received corresponds to the code sent (user verification), the information processing system (26, 30) authorizes the user to send a

message (a bank transfer or a telephone call) to a recipient.

3. By contrast, the authentication routine according to D1 does not use this method (sending and receipt of a unique code on two different transmission media) in order to verify the *recipient* of the transfer or telephone call.
A novel contribution is therefore made by the method claimed in the present application: the information processing system opens a communication session with a remote communication means, corresponding to the recipient, and during said communication session [i.e. with the recipient], the information processing system sends and receives the unique code (= first piece of so-called confidential information for one-time use) in order to ensure that it complies. Thus, the security of the communication between the information processing system and the recipient's communication means can be examined (before supplying a secure message to the recipient).

The documents published before the priority date of the present application do not anticipate this method.

4. By contrast, an obvious variation of the system of D1 comprises producing the information processing system (26, 30) in the form of a server in a communication network. In that case, a user cannot only search for data in the information processing system but he can also store there (i.e. on the server) data (for example a message) intended for a second user (recipient). When the second user

searches for these data through the network, his identity is normally verified before the stored message is supplied to him. It goes without saying that the recipient can be verified according to the same process, which is described in the context of checking the first user at the time of storage (unique code on two media).

Given that Claim 1 encompasses the method which has just been deduced in an obvious manner from the prior art, Claim 1 does not meet the requirements of PCT Article 33(3) and PCT Rule 65.

5. The device according to independent Claim 9 is based on the same concept as the method according to Claim 1. Consequently, the assessment of Claim 9 is the same as for Claim 1.

6. The dependent claims do not add any features which, in combination with the subject matter of the independent claims, would involve an inventive step.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: VI

Certain documents

7. The prior art document GB-A-2 328 310 (D2) was filed (14 May 1997) before the priority date (4 November 1997) claimed by the international application, and D2 was published (17 February 1999) after the filing date of the international application (3 November 1998). The examiner also observes that the United Kingdom has been designated in the international application.

D2 relates to an identification method equivalent to that of D1; an information processing system (central computer) transmits a single-use code ("one time, non-predictable code") to a user (paging receiver) on a first transmission medium (broadcast system, paging E signal). The user sends the (converted) code back to the information processing system (central computer) on a second transmission medium (Internet) so that said system can check that the codes comply and thus establish the user's identity (D2, page 5, paragraph 2 to page 6, paragraph 4).

In addition, D2 (page 8, last paragraph to page 9, first paragraph) envisages a situation where the identity of two users is verified. Messages ("details of the transaction information") are sent to a bank clerk. The details of the transaction can only be transmitted by at least one of the users.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: VI

Furthermore, both users receive the data on their respective devices (page 9, line 1), which means that each user is also the recipient of the messages. Given that each user/recipient is examined by means of a respective unique code (D2, page 9, line 2) transmitted on two different transmission media (pager-based broadcast system [page 4, last paragraph]; Internet [page 6, lines 9 to 12]), D2 anticipates at the national level in the United Kingdom a method comprising all the steps defined in Claim 1 of the present international application and a device (according to Claim 9) for implementing the method.

8. The examiner has not had the opportunity to verify the document (FR 97/13825) whose priority date (4 November 1997) is claimed by the present international application. Consideration should therefore be given to prior art document NL-C-1 007 409 (D3), which was published in the priority period of the international application. The examiner also observes that the Netherlands has been designated in the international application.

D3 provides a method for authenticating a local user (2) of an information processing system (3) (D3, Claims 1 and 4). For that purpose, an authentication server (4) generates a random code (page 2, lines 6 and 7) and sends it to the local terminal (2) and to the system (3) which requests user authentication. When the user sends his code

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: VI

to the system (3), the system compares the codes received in order to verify the authentication. The codes can be transmitted through several media. The server (4) can form part of the system (3) (D3, page 2, lines 22 and 23).

By contrast, D3 does not describe the transmission of a message from a user to a recipient via an information processing system so that said system verifies the identity of the recipient via two transmission media.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

9. In order to satisfy the requirements of PCT Rule 5.1(a)(ii), at least document D1 should have been additionally cited in the introductory part of the description.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

10. The introductory part of the description should have been brought into line with the amended set of claims (PCT Article 6; PCT Rule 5.1(a)(iii)).

WO 99/23617
PCT/FR98/02348

TRAITE DE COOPERATION EN MATIERE DE BREVETS

Expéditeur: le BUREAU INTERNATIONAL

PCT

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

(règle 47.1.c), première phrase, du PCT)

Destinataire:
KREMER, Gilles
34, avenue de la Paix
F-92170 Vanves
FRANCE

Date d'expédition (jour/mois/année) 14 mai 1999 (14.05.99)	
Référence du dossier du déposant ou du mandataire	**AVIS IMPORTANT**

Demande internationale no	Date du dépôt international (jour/mois/année)	Date de priorité (jour/mois/année)
PCT/FR98/02348	03 novembre 1998 (03.11.98)	04 novembre 1997 (04.11.97)

Déposant
KREMER, Gilles etc

1. Il est notifié par la présente qu'à la date indiquée ci-dessus comme date d'expédition de cet avis, le Bureau international a communiqué, comme le prévoit l'article 20, la demande internationale aux offices désignés suivants:
   AU,CN,EP,IL,JP,KP,KR,US

   Conformément à la règle 47.1.c), troisième phrase, ces offices acceptent le présent avis comme preuve déterminante du fait que la communication de la demande internationale a bien eu lieu à la date d'expédition indiquée plus haut, et le déposant n'est pas tenu de remettre de copie de la demande internationale à l'office ou aux offices désignés.

2. Les offices désignés suivants ont renoncé à l'exigence selon laquelle cette communication doit être effectuée à cette date:
   AL,AM,AP,AT,AZ,BA,BB,BG,BR,BY,CA,CH,CU,CZ,DE,DK,EA,EE,ES,FI,GB,GE,GH,GM,HR,HU,ID,
   IS,KE,KG,KZ,LC,LK,LR,LS,LT,LU,LV,MD,MG,MK,MN,MW,MX,NO,NZ,OA,PL,PT,RO,RU,SD,SE,SG,
   SI,SK,SL,TJ,TM,TR,TT,UA,UG,UZ,VN,YU,ZW
   La communication sera effectuée seulement sur demande de ces offices. De plus, le déposant n'est pas tenu de remettre de copie de la demande internationale aux offices en question (règle 49.1)a-bis)).

3. Le présent avis est accompagné d'une copie de la demande internationale publiée par le Bureau international le
   14 mai 1999 (14.05.99) sous le numéro WO 99/23617

RAPPEL CONCERNANT LE CHAPITRE II (article 31.2)a) et règle 54.2)

Si le déposant souhaite reporter l'ouverture de la phase nationale jusqu'à 30 mois (ou plus pour ce qui concerne certains offices) à compter de la date de priorité, **la demande d'examen préliminaire international** doit être présentée à l'administration compétente chargée de l'examen préliminaire international avant l'expiration d'un délai de 19 mois à compter de la date de priorité.

Il appartient exclusivement au déposant de veiller au respect du délai de 19 mois.

Il est à noter que seul un déposant qui est ressortissant d'un Etat contractant du PCT lié par le chapitre II ou qui y a son domicile peut présenter une demande d'examen préliminaire international.

RAPPEL CONCERNANT L'OUVERTURE DE LA PHASE NATIONALE (article 22 ou 39.1))

Si le déposant souhaite que la demande internationale procède en phase nationale, il doit, dans le délai de 20 mois ou de 30 mois, ou plus pour ce qui concerne certains offices, accomplir les actes mentionnés dans ces dispositions auprès de chaque office désigné ou élu.

Pour d'autres informations importantes concernant les délais et les actes à accomplir pour l'ouverture de la phase nationale, voir l'annexe du formulaire PCT/IB/301 (Notification de la réception de l'exemplaire original) et le volume II du Guide du déposant du PCT.

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé
J. Zahra

no de téléphone (41-22) 338.83.38

Suite du formulaire PCT/IB/308

AVIS INFORMANT LE DEPOSANT DE LA COMMUNICATION DE LA DEMANDE INTERNATIONALE AUX OFFICES DESIGNES

Date d'expédition (jour/mois/année) 14 mai 1999 (14.05.99)	AVIS IMPORTANT
Référence du dossier du déposant ou du mandataire	Demande internationale no PCT/FR98/02348

Il est notifié au déposant que, au moment de l'établissement du présent avis, le délai fixé à la règle 46.1 pour le dépôt de modifications selon l'article 19 n'était pas encore expiré et que le Bureau international n'avait pas reçu de modications ni de déclaration l'informant que le déposant ne souhaitait pas présenter de modifications.

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire ./.	**POUR SUITE A DONNER** voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR98/02348	Date du dépot international *(jour/mois/année)* 03/11/1998	Date de priorité *(jour/mois/année)* 04/11/1997
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G07F7/10		
Déposant KREMER, Gilles et al.		

1. Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.

2. Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.

   ☒ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

   Ces annexes comprennent 3 feuilles.

3. Le présent rapport contient des indications relatives aux points suivants:

I	☒	Base du rapport
II	☐	Priorité
III	☐	Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
IV	☐	Absence d'unité de l'invention
V	☒	Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
VI	☐	Certains documents cités
VII	☒	Irrégularités dans la demande internationale
VIII	☒	Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale	Date d'achèvement du présent rapport
03/06/1999	14.02.00
Nom et adresse postale de l'administration chargée de l'examen préliminaire international: Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Bumes, K N° de téléphone +49 89 2399 2393

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

Demande internationale n° PCT/FR98/02348

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1-47 version initiale

Revendications, N°:

1-10 reçue(s) avec télécopie du 02/02/2000

Dessins, feuilles:

1/13-13/13 version initiale

2. Les modifications ont entrainé l'annulation :

☐ de la description, pages :
☒ des revendications, n°s : 11-29
☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

voir feuille séparée

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui :	Revendications	1-10
	Non :	Revendications	
Activité inventive	Oui :	Revendications	
	Non :	Revendications	1-10
Possibilité d'application industrielle	Oui :	Revendications	1-10
	Non :	Revendications	

2. Citations et explications

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :

voir feuille séparée

VIII. Observations relatives à la demande internationale

Les observations suivantes sont faites au sujet de la clarté des revendications, de la description et des dessins et de la question de savoir si les revendications se fondent entièrement sur la description :

voir feuille séparée

I. Base de l'opinion

Exposé initial des revendications modifiées

1. Le procédé selon la revendication 1 modifiée se fonde notamment sur les modes de réalisation décrits en liaison avec les figures 4 à 8.

   Le dispositif selon la revendication 9 met en oeuvre le procédé revendiqué et n'étend pas l'enseignement technique de la demande telle que déposée.

V. Citations et explications à l'appui de la déclaration quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

2. WO-A-96/00485 (D1) décrit un procédé de transmission de message dans lequel un utilisateur (figure 1: personal unit 20, terminal 22) entre en contact avec un système de traitement d'information (service node 26, en combinaison avec un centre d'authentification 30 - voir la page 5, lignes 14 à 26).

   Avant de fournir la prestation voulue (home banking, D1, page 12, ligne 21 à la page 13, ligne 20; comptabilisation pour les coups de téléphone, D1, page 13, ligne 21 à la page 14, ligne 3), le système de traitement d'information met en oeuvre une routine d'authentification (D1, page 9, ligne 1 à la page 12, ligne 20) au cours de laquelle le système de traitement d'information
   - envoie un code unique (page 7, ligne 32) à l'utilisateur (20, 22) sur un premier support de transmission (authentication challenge network 28), et
   - reçoit le code unique depuis l'utilisateur sur un deuxième support de transmission (service access network 24).

   Si le code reçu correspond au code envoyé (vérification de l'utilisateur), le système de traitement d'information (26, 30) autorise l'utilisateur à envoyer un message (un virement de banque ou un coup de téléphone) à un destinataire.

3. Par contre, la routine d'authentification selon D1 n'emploie pas ce procédé (envoi et réception d'un code unique sur deux supports de transmission différents) pour vérifier le *destinataire* du virement ou du coup de téléphone.

Il s'agit donc d'un nouvel apport du procédé revendiquée dans la présente demande: Le système de traitement d'information ouvre une session de communication avec un moyen de communication situé à distance, correspondant au destinataire, et durant ladite session de communication [c'est-à-dire avec le destinataire], le système de traitement d'information envoie et reçoit le code unique (= première information dite confidentielle à usage unique) pour en vérifier la conformité. De cette façon, la sécurité de la communication entre le système de traitement d'information et le moyen de communication du destinataire peut être examinée (avant de fournir un message sécurisé au destinataire).

Les documents qui ont été publiés avant la date de priorité de la présente demande n'antériorisent pas cette approche.

4. Par contre, une variation évidente du système de D1 consiste à réaliser le système de traitement d'information (26, 30) sous forme de serveur dans un réseau de communication. Dans ce cas-là, un utilisateur ne peut pas seulement chercher des données dans le système de traitement d'information mais il peut aussi y stocker (sur le serveur) des données (par exemple un message) à l'intention d'un deuxième utilisateur (destinataire). Lorsque le deuxième utilisateur vient chercher ces données à travers le réseau, il est normal que son identité soit vérifiée avant que le message stocké lui soit fourni. Il va de soi que la vérification du destinataire peut se dérouler selon le même schéma qui est décrit pour vérifier le premier utilisateur lors du stockage (code unique sur deux supports).

   Étant donné que la revendication 1 englobe le procédé qui vient d'être déduit de l'état de la technique de façon évidente, la revendication 1 ne remplit pas les conditions énoncées à l'article 33 (3) et la règle 65 PCT.

5. Le dispositif selon la revendication indépendante 9 repose sur le même concept que le procédé selon la revendication 1. Par conséquent, la revendication 9 est appréciée de la même manière que la revendication 1.

6. Les revendications dépendantes ne rajoutent pas de caractéristique qui, en combinaison avec l'objet des revendications indépendantes, impliquerait une activité inventive.

VI. Certains documents

7. L'antériorité GB-A-2 328 310 (D2) a été déposée (14.05.97) avant la date de priorité (04.11.97) revendiquée par la demande internationale, et D2 a été publiée (17.02.99) après la date de dépôt de la demande internationale (03.11.98). L'examinateur observe aussi que Le Royaume Uni a été désigné dans la demande internationale.

D2 porte sur un procédé d'identification équivalent à celui de D1: Un système de traitement d'information (central computer) transmet un code à usage unique ("one time, non-predictable code") vers un utilisateur (paging receiver) sur un premier support de transmission (broadcast system, paging E signal). L'utilisateur renvoie le code (transformé) vers le système de traitement d'information (central computer) sur un deuxième support de transmission (internet) pour que le système de traitement d'information puisse vérifier la conformité des codes et établir ainsi l'identité de l'utilisateur (D2, page 5, paragraphe 2 à la page 6, paragraphe 4).

En outre, D2 (page 8, dernier paragraphe à la page 9, premier paragraphe) envisage un cas de figure où l'identité de deux utilisateurs est vérifiée: Des messages ("details of the transaction information") sont envoyés à un employé de banque. Les détails de la transaction ne peuvent être transmis que par au moins un des utilisateurs.

En plus, les deux utilisateurs reçoivent les données sur leur dispositif respectif (page 9, ligne 1) ce qui signifie que chaque utilisateur est aussi destinataire des messages. Etant donné que chaque utilisateur/destinataire est examiné à l'aide d'un code unique respectif (D2, page 9, ligne 2) transmis sur deux supports de transmission différents (pager-based broadcast system [page 4, dernier alinéa]; internet [page 6, lignes 9 à 12]), D2 antériorise, au niveau national britannique, un procédé comprenant toutes les étapes définies dans la revendication 1 de la présente demande internationale et un dispositif (selon la revendication 9) pour mettre en oeuvre le procédé

8. L'examinateur n'a pas eu l'occasion de vérifier le document (FR 97/13825) dont la la date de priorité (04.11.97) est revendiquée par la présente demande internationale. Il faut donc prendre en compte l'antériorité NL-C-1 007 409 (D3) qui a été publiée dans l'intervalle de priorité de la demande internationale. L'examinateur observe aussi que les Pays-Bas ont été désignés dans la demande internationale.

D3 prévoit un procédé d'authentification d'un utilisateur local (2) face à un système de traitement d'information (3) (D3, revendications 1 et 4). Dans ce but, un serveur d'authentification (4) engendre un code aléatoire (page 2, lignes 6/7) et l'envoie au terminal local (2) et au système (3) qui demande l'authentification de l'utilisateur. Lorsque l'utilisateur envoie son code au système (3), celui-ci compare les codes reçus pour vérifier l'authentification. Les codes peuvent être transmis à travers plusieurs médias. Le serveur (4) peut faire partie du système (3) (D3, page 2, lignes 22/23).

Par contre, D3 ne décrit pas la transmission d'un message depuis un utilisateur vers un destinataire par l'intermédiaire d'un système de traitement d'information de façon à ce que le système de traitement d'information vérifie l'identité du destinataire à travers deux supports de transmission.

VII. Irrégularités dans la demande internationale

9. En vue de satisfaire aux conditions énoncées à la règle 5.1 (a) (ii) PCT, il y aurait eu lieu de citer additionnellement dans la partie introductive de la description au moins le document D1.

VIII. Observations relatives à la demande internationale

10. Il y aurait eu lieu d'harmoniser la partie introductive de la description avec le jeu de revendications modifié (article 6; règle 5.1 (a) (iii) PCT).

* * *

REVENDICATIONS

1. Procédé de transmission d'un message électronique sécurisé comportant :

- une opération de réception par un système de traitement d'information, en provenance d'un utilisateur, par l'intermédiaire d'un réseau de communication :

. du message à transmettre,

. d'un identifiant de l'utilisateur, et

. d'un identifiant d'un destinataire dudit message (603, 604) ;

- une opération d'ouverture d'une session de communication entre un moyen de communication situé à distance correspondant à l'identifiant du destinataire dudit message, et le système de traitement d'information ;

- une opération de génération, par ledit système de traitement d'information, d'une première information dite « confidentielle » à usage unique, c'est-à-dire ne pouvant être utilisée que pendant ladite session de communication ;

et, durant ladite session de communication :

. une opération de transmission, par le système de traitement d'information, de la première information confidentielle par l'intermédiaire d'un premier support de transmission (605),

. une opération de réception, par le système de traitement d'information, de ladite première information confidentielle en provenance d'un deuxième support de transmission différent du premier support de transmission (608),

. une opération de vérification de la première information confidentielle (610), par ledit système de traitement d'information, et

. si la première information confidentielle est vérifiée, une opération de fourniture du message sécurisé, par le système de traitement d'information, au moyen de communication situé à distance correspondant à l'identifiant du destinataire dudit message.

2. Procédé selon la revendication 1, caractérisé en ce qu'il comporte, en outre, une opération d'information dudit utilisateur de la fourniture du message sécurisé audit destinataire.

3. Procédé selon l'une quelconque des revendications 1 ou 2, caractérisé en ce qu'il comporte, en outre, une opération d'authentification dudit utilisateur.

4. Procédé selon la revendication 3, caractérisé en ce que la dite opération d'authentification dudit utilisateur comporte :

- une opération de génération, par ledit système de traitement d'information, d'une deuxième information dite « confidentielle » à usage unique;

- une opération de fourniture audit utilisateur, par ledit système de traitement d'information, de la deuxième information confidentielle, sur un troisième support de transmission (605),

- une opération de réception, par le système de traitement d'information, de la deuxième information confidentielle, sur un quatrième support de transmission différent du troisième support de transmission (608),

- une opération de vérification de la deuxième information confidentielle (610) par ledit système de traitement d'information.

5. Procédé selon la revendication 4, caractérisé en ce qu'il comporte, en outre, une opération de délivrance audit destinataire d'un certificat qui identifie ledit utilisateur.

6. Procédé selon l'une quelconque des revendications 1 à 5, caractérisé en ce qu'il comporte une opération de mise en mémoire d'au moins une trace d'au moins une opération, dans le système de traitement d'information.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le premier support de transmission est un support sans fil.

8. Procédé selon l'une quelconque des revendications 1 à 7, caractérisé en ce que le deuxième support de transmission est l'Internet.

9. Dispositif de transmission d'un message électronique sécurisé comportant des moyens de traitement adaptés à :

- recevoir en provenance d'un utilisateur, par l'intermédiaire d'un réseau de communication :

. le message à transmettre,

. un identifiant de l'utilisateur, et

. un identifiant d'un destinataire dudit message (603, 604);

- ouvrir une session de communication avec un moyen de communication situé à distance correspondant à l'identifiant du destinataire dudit message ;

- générer une première information dite « confidentielle » à usage unique, c'est-à-dire ne pouvant être utilisée que pendant ladite session de communication ;

et, durant ladite session de communication :

. transmettre la première information confidentielle par l'intermédiaire d'un premier support de transmission (605),

. recevoir ladite première information confidentielle en provenance d'un deuxième support de transmission différent du premier support de transmission (608),

. vérifier la première information confidentielle (610), et

. si la première information confidentielle est vérifiée, fournir le message sécurisé audit destinataire, par l'intermédiaire d'un support de transmission.

10. Dispositif selon la revendication 9, caractérisé en ce que les moyens de traitement sont adaptés, en outre, à transmettre une information audit utilisateur de la fourniture du message sécurisé audit destinataire.

CLAIMS

1. Process for the transmission of information on a first communication support, characterized in that it comprises:

- an operation of opening a communication session with a remote communication means, on said first communication support,

and, during said session:

. performing an operation of receiving confidential information on a terminal with a unique address on a second communication support, and

. performing an operation of transmission, on the first communication support, of a confidential message representative of said confidential information.

2. Process for the transmission of information on a first communication support, characterized in that it comprises:

- an operation of opening, by means of a unique address terminal on said first communication support, a communication session with a remote communication means,

and, during said session:

. performing an operation of reception of confidential information on the first communication support, and

. performing an operation of transmission, on a second communication support, of a confidential message representative of said confidential information.

3. Process for the transmission of information on a first communication support, characterized in that it comprises:

- an operation of opening, by means of a first terminal, a communication session with a remote communication means, on said first communication support,

- an operation of opening, by means of a second terminal, of a communication session with a remote communication means, on a second communication support,

- when the two sessions are open, performing an operation of reception of confidential information on one of said communication supports on which one of the terminals has a unique address, and

- performing an operation of transmission, on the other of said communication supports, of a confidential message representative of said confidential information.

4. Process for the transmission of information on a first communication support, characterized in that it comprises:

- an operation of opening a communication session with a remote communication means, on said first communication support,

and, during said session:

. performing an operation generating confidential information and transmitting said confidential information, to a terminal with a unique address on a second support,

. performing an operation of receiving, on the first communication support, a confidential message adapted to be representative of said confidential information, and

. performing an operation of verifying the correspondence between said confidential message and said confidential information.

5. Process for the transmission of information on a so-called "second" communication support, said communication support forming a part of a communication network, characterized in that it comprises:

- an operation of receiving, from a so-called "second" terminal, a first message representative:

. of an identification of a so-called "third" terminal having a unique address on said network,

. of confidential information,

. of information representative of the amount of a transaction,

- performing a transmission operation, to the third terminal, of a second message representative:

. of said confidential information and

. of said amount,

- performing an operation of receiving a third message, from said second terminal, representative of a validation of a transaction, and

- performing an operation of incrementing a register corresponding to said third terminal, by a value representative of a duration of the first session.

6. Process for the transmission of information on a so-called "second" communication support, said communication support forming a part of a communication network, characterized in that it comprises:

- an operation of receiving, from a so-called "second" terminal, of a first message representative:

. of the identification of a so-called "third" terminal having a unique address on said network,

. of confidential information,

. of information representative of the amount of a transaction,

- performing an operation of transmission, to the third terminal, of a second message representative:

. of said confidential information and

. of said amount,

- performing an operation of incrementing a register corresponding to said third terminal, by a predetermined value.

7. Process for the transmission of information on a so-called "second" communication support, said communication support forming a part of a communication network, characterized in that it comprises:

- an operation of receiving, from a so-called "second" terminal, a first message representative:

. of an identification of a so-called "third" terminal having a unique address on said network,

. of confidential information,

. of information representative of an amount of a transaction,

- performing an operation of transmitting, to the third terminal, of a second message representative:

. of said confidential information and

. of said amount,

- performing an operation of receiving a third message, from said second terminal, representative of the validation of a transaction, and

- performing an operation of incrementing a register corresponding to said third terminal, by a value representative of said amount of the transaction.

8. Process for the transmission of information, between a first and a second terminal, on a first communication support belonging to a communication network, characterized in that it comprises:

- an operation of opening a communication session, on the first communication support, between the first and the second terminal, and

- an operation of transmission, from the second terminal to a third terminal connected to a second network and having a unique address on said second network, of a first message representative of confidential information,

- an operation of transmission, to an address on said network which corresponds to said third terminal, of a second message representative of said confidential information, and

- an operation of transmission, on the first communication support, from the first terminal and to the second terminal, of a message representative of the confidential information.

9. Process for the transmission of information on a first communication support forming a part of a communication network, characterized in that it comprises:

- an operation of receiving, from a first terminal, a first message representative:

. of an amount of a contemplated transaction,

. of an identification of a debtor,

- an operation of transmission, on a second communication support, to a bank server, of a second message representative:

. of said amount,

. of an identification of a debtor

. of a request for authorization of a debit,

- an operation of reception or not by the said bank server, of a third message representative of an authorization of a debit,

- when the authorization is given, an operation of transmission, to a second terminal having a unique address on a second communication network, of a fourth message representative of confidential information,

- an operation of receiving, from said first terminal, a fifth message representative of said confidential information,

- an operation of verification of the correspondence between the confidential message and the confidential information.

10. Process for the transmission of information on a first communication support forming a part of a communication network, characterized in that it comprises:

- an operation of receiving, from a first terminal, a first message representative:

. of an amount of a contemplated transaction,

. of an identification of a debtor,

- an operation of authorizing or not, a debit to a bank account,

- when the authorization is given, an operation of transmission, to a second terminal having a unique address on a second communication network, of a second message representative of the confidential information,

- an operation of receiving, from said first terminal, a third message representative of said confidential information,

- an operation of verifying the correspondence between the confidential message and the confidential information and

- in the case in which the correspondence is verified, an operation of debiting said amount to said bank account.

11. Process for the transmission of information according to any one of claims 1 to 10, characterized in that

the confidential information is representative of a session number attributed to said session.

12. Process for the transmission of information according to any one of claims 1 to 11, characterized in that the confidential information is representative of a pseudo-random number.

13. Process for the transmission of information according to any one of claims 1 to 12, characterized in that the confidential information is representative of the time and date of said operation of opening the session.

14. Process for the transmission of information according to any one of claims 1 to 13, characterized in that the confidential information is representative of an identification of the user.

15. Process for the transmission of information according to any one of claims 1 to 14, characterized in that the confidential information is modified at each of the sessions.

16. Process for the transmission of information according to any one of claims 1 to 15, characterized in that the confidential information is representative of one or several bank account numbers and/or money card numbers.

17. Process of transmission according to any one of claims 1 to 16, characterized in that, in the course of the operation of receiving confidential information, there is moreover received an amount of the transaction.

18. Process for transmission according to any one of claims 1 to 17, characterized in that, in the course of the operation of transmission of a confidential message representative of confidential information, there is moreover transmitted an amount of the transaction.

19. Process for transmission according to claim 9, characterized in that after the operation of verification of correspondence, in the case of correspondence, it comprises an operation of incrementing a debit account of said debtor.

20. Process of transmission according to any one of claims 9 or 19, characterized in that it comprises, after the operation of receiving the first message, a reading operation, from a database, of the unique address of the second terminal in the second network.

21. Process for transmission according to any one of claims 9, 19 or 20, characterized in that it comprises, after the operation of receiving the first message, a reading operation, from the database, of an identification of said bank server.

22. Process for transmission according to any one of claims 1 to 21, characterized in that it comprises an operation of manually acquiring, in the course of which the user acquires a confidential message representative of the confidential information.

23. Process for transmission according to any one of claims 1 to 22, characterized in that it comprises an operation of transmission of selection, in the course of which, as a function of predetermined criteria, the transmissions are classified into two groups, are relating to the so-called "to be secured" transmissions and the others to the so-called "normal" transmissions, the normal transmissions not giving rise to more than one transmission operation on one communication support.

24. Process for transmission according to claim 23, characterized in that, in the course of said selection operation, there is used a transaction limit amount, the so-called "to be secured" transactions being those with which are associated amounts of transaction greater than said limit amount.

25. Process for transmission according to any one of claims 1 to 24, characterized in that it comprises an operation of transmission of a unique address on one of said networks.

26. Process for transmission according to claim 25, characterized in that, in the course of said transmission operation of a unique address, a certificate is transmitted containing information representative of said unique address.

27. Process for transmission according to claim 26, characterized in that said certificate responds to a security protocol for payment and comprises information representative of said unique address.

28. Computer server, characterized in that it is adapted to use the transmission process according to any one of claims 1 to 27.

29. Computer, characterized in that it is adapted to use the process of transmission according to any one of claims 1 to 27.

30. Process for the transmission of a secured electronic message, comprising:

- an operation of receiving by an information processing system, from a user, by means of a communication network:

. the message to be transmitted,

. an identification of the user, and

. an identification of a destination for said message (603, 604);

- an operation of opening a communication session between a remotely located communication means corresponding to the identification of the destination of said message, and the information processing system;

- an operation of generating, by said information processing system, a first so-called "confidential" information for single use, which is to say being able to be used only during said communication session;

and, during said communication session:

. an operation of transmission, by the information processing system, of the first confidential information by means of a first transmission support (605),

. an operation of receiving, by the information processing system, of said first confidential information from a second transmission support different from the first transmission support (608),

. an operation of verification of the first confidential information (610), by said information processing system, and

. if the first confidential information is verified, an operation of supplying the secured message, by the information processing system, to the remotely located communication means corresponding to the identification of the destination of said message.

PCT ORGANISATION MONDIALE DE LA PROPRIETE INTELLECTUELLE
Bureau international

DEMANDE INTERNATIONALE PUBLIEE EN VERTU DU TRAITE DE COOPERATION EN MATIERE DE BREVETS (PCT)

(51) Classification internationale des brevets 6 : G07F 7/00

A2

(11) Numéro de publication internationale: WO 99/23617

(43) Date de publication internationale: 14 mai 1999 (14.05.99)

(21) Numéro de la demande internationale: PCT/FR98/02348

(22) Date de dépôt international: 3 novembre 1998 (03.11.98)

(30) Données relatives à la priorité:
97/13825 4 novembre 1997 (04.11.97) FR

(71)(72) Déposants et inventeurs: KREMER, Gilles [FR/FR]; 34, avenue de la Paix, F–92170 Vanves (FR). CHANUDET, Patrick [FR/FR]; 17 bis, rue de la Station, F–92600 Asnières (FR).

(74) Représentant commun: KREMER, Gilles; 34, avenue de la Paix, F–92170 Vanves (FR).

(81) Etats désignés: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, brevet ARIPO (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Publiée

Sans rapport de recherche internationale, sera republiée dès réception de ce rapport.

(54) Title: METHOD FOR TRANSMITTING DATA AND IMPLEMENTING SERVER

(54) Titre: PROCEDE DE TRANSMISSION D'INFORMATION ET SERVEUR LE METTANT EN OEUVRE

(57) Abstract

The invention concerns the combined use of at least two communication networks and more precisely confidential data exchange to a first data medium user by means of a second data medium via a mechanism synchronising the data media and sending data from one medium to the other. The data transmission method on a first medium thus consists in: an operation for opening a communication session with means of communication remotely located, on said first communication medium; and during said session: an operation for receiving confidential information on a single address terminal on a second communication medium; and an operation for transmitting, on the first communication medium, a confidential message representing the confidential information; an operation for verifying whether the confidential message corresponds to the confidential information.

(57) Abrégé

La présente invention propose l'utilisation combinée d'au moins deux réseaux de communication et plus précisément l'échange d'information confidentielle à un usager d'un premier support d'information à l'aide d'un deuxième support d'information par l'intermédiaire d'un mécanisme de synchronisation des supports d'information et de renvoi d'information d'un support à l'autre. Le procédé de transmission d'information sur un premier support comporte ainsi: une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de communication, et, durant ladite session: une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de communication, et une opération de transmission, sur le premier support de communication, d'un message confidentiel représentant l'information confidentielle, une opération pour vérifier si le message confidentiel correspond à l'information confidentielle.

UNIQUEMENT A TITRE D'INFORMATION

Codes utilisés pour identifier les Etats parties au PCT, sur les pages de couverture des brochures publiant des demandes internationales en vertu du PCT.

AL	Albanie	ES	Espagne	LS	Lesotho	SI	Slovénie
AM	Arménie	FI	Finlande	LT	Lituanie	SK	Slovaquie
AT	Autriche	FR	France	LU	Luxembourg	SN	Sénégal
AU	Australie	GA	Gabon	LV	Lettonie	SZ	Swaziland
AZ	Azerbaïdjan	GB	Royaume-Uni	MC	Monaco	TD	Tchad
BA	Bosnie-Herzégovine	GE	Géorgie	MD	République de Moldova	TG	Togo
BB	Barbade	GH	Ghana	MG	Madagascar	TJ	Tadjikistan
BE	Belgique	GN	Guinée	MK	Ex-République yougoslave de Macédoine	TM	Turkménistan
BF	Burkina Faso	GR	Grèce			TR	Turquie
BG	Bulgarie	HU	Hongrie	ML	Mali	TT	Trinité-et-Tobago
BJ	Bénin	IE	Irlande	MN	Mongolie	UA	Ukraine
BR	Brésil	IL	Israël	MR	Mauritanie	UG	Ouganda
BY	Bélarus	IS	Islande	MW	Malawi	US	Etats-Unis d'Amérique
CA	Canada	IT	Italie	MX	Mexique	UZ	Ouzbékistan
CF	République centrafricaine	JP	Japon	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Pays-Bas	YU	Yougoslavie
CH	Suisse	KG	Kirghizistan	NO	Norvège	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	République populaire démocratique de Corée	NZ	Nouvelle-Zélande		
CM	Cameroun			PL	Pologne		
CN	Chine	KR	République de Corée	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Roumanie		
CZ	République tchèque	LC	Sainte-Lucie	RU	Fédération de Russie		
DE	Allemagne	LI	Liechtenstein	SD	Soudan		
DK	Danemark	LK	Sri Lanka	SE	Suède		
EE	Estonie	LR	Libéria	SG	Singapour		

PROCEDE DE TRANSMISSION D'INFORMATION ET SERVEUR LE METTANT EN OEUVRE

La présente invention concerne un procédé de transmission d'information et un serveur informatique le mettant en oeuvre. Elle permet de s'assurer que la personne opérant depuis un terminal est une personne autorisée ou habilitée. Elle s'applique, en particulier, à la vérification d'identité de la personne qui accède à un service distant, quel que soit le terminal utilisé. Elle permet d'authentifier l'identité de l'utilisateur, d'authentifier une transaction, de vérifier l'intégrité de cette transaction en la complétant du montant de ladite transaction, de la quantité achetée, du nom du produit ou du service acquis, et ainsi de permettre le paiement de biens ou de services, en ligne, c'est-à-dire au cours d'une communication entre systèmes informatiques distants.

Des domaines d'application de l'invention sont, par exemple, le contrôle d'accès, la remise en main propre d'information confidentielle, la certification de transactions ou de paiement de biens ou services sur un réseau informatique.

La mise en œuvre de la transaction à distance sur réseau pose, indépendamment de l'encryptage, le problème de l'authentification de la personne qui la réalise, de l'intégrité de la transaction et de sa confidentialité. Dans de nombreuses applications (commerce électronique, banque à distance, télé travail, sécurité interne des entreprises, sécurisation de bases de données payantes, par exemple) et sur tous supports (réseaux informatiques locaux ou distants, par exemple, respectivement, les réseaux communément appelés «intranet» ou «internet», serveurs vocaux, par exemple), ce problème est crucial.

Les dispositifs et procédés de sécurisation connus dans l'art antérieur comme ceux illustrés dans le document US-A-5.442.704, qui utilisent une carte à mémoire, imposent des contraintes matérielles importantes et coûteuses.

D'autres dispositifs logiciels, basés sur des systèmes d'encryptage assurent la confidentialité des données sans garantir l'authentification de la personne.

D'autres dispositifs utilisent un moyen d'authentification, connu sous le nom «d'authentifieur» ou de «token», qui calcule à partir de données reçues au cours d'une transaction et d'une clé secrète qu'il conserve en mémoire, un mot de passe dynamique. Ces dispositifs imposent, de nouveau, des contraintes matérielles importantes et coûteuses.

La présente invention entend remédier à ces inconvénients. A cet effet, la présente invention propose l'utilisation combinée d'au moins deux réseaux de communication.

En d'autres termes, la présente invention propose la transmission, à un usager d'un premier support de communication, d'une information confidentielle, sur un deuxième support d'information, préférentiellement sécurisé, avec :

- un mécanisme de synchronisation des deux communications sur les deux réseaux et

- une opération de renvoi, d'un support de communication à l'autre, à l'initiative de l'usager, par saisie préférentiellement manuelle, de l'information confidentielle reçue sur l'autre support.

A cet effet, la présente invention vise, selon un premier aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de transmission, et

. une opération de transmission, sur le premier support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un deuxième aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un terminal à adresse unique sur ledit premier support de transmission, d'une session de communication avec un moyen de communication situé à distance,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur le premier support de transmission, et

. une opération de transmission, sur un deuxième support de transmission, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un troisième aspect, un procédé de transmission d'information sur un premier support de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un premier terminal, d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de communication,

- une opération d'ouverture, par l'intermédiaire d'un deuxième terminal, d'une session de communication avec un moyen de communication situé à distance, sur un deuxième support de communication,

- lorsque les deux sessions sont ouvertes, une opération de réception d'une information confidentielle sur un desdits supports de communication sur lequel l'un des terminaux a une adresse unique, et

- une opération de transmission, sur l'autre desdits supports de communication, d'un message confidentiel représentatif de ladite information confidentielle.

La présente invention vise, selon un quatrième aspect, un procédé de transmission d'information sur un premier support de transmission, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de transmission,

et, durant ladite session :

. une opération de génération d'une information confidentielle et de transmission de ladite information confidentielle sur un deuxième support de transmission à un terminal possédant une adresse unique sur le deuxième support,

. une opération de réception, sur le premier support de transmission, d'un message confidentiel susceptible d'être représentatif de ladite information confidentielle, et

. une opération de vérification de correspondance entre ledit message confidentiel et ladite information confidentielle.

La présente invention vise, selon un cinquième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative dudit montant de transaction.

La présente invention vise, selon un sixième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit

support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :
  - . d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,
  - . d'une information confidentielle,
  - . d'une information représentative d'un montant de transaction,
- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :
  - . de ladite information confidentielle et
  - . dudit montant,
- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et
- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative d'une durée de la première session.

On observe que, selon les cinquième et sixième aspects, de l'invention, l'opération d'incrémentation peut avoir lieu avant ou après l'opération de réception d'un troisième message.

La présente invention vise, selon un septième aspect, un procédé de transmission d'information sur un support de transmission dit "deuxième", ledit support de transmission faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :
  - . d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,
  - . d'une information confidentielle,
  - . d'une information représentative d'un montant de transaction,
- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :
  - . de ladite information confidentielle et

. dudit montant,

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur prédéterminée.

La présente invention vise, selon un huitième aspect, un procédé de transmission d'information, entre un premier terminal et un deuxième terminal, sur un premier support de transmission appartenant à un réseau de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture de session de communication, sur le premier support de transmission entre le premier terminal et le deuxième terminal, et

- une opération de transmission, de la part du deuxième terminal à un troisième terminal raccordé à un deuxième réseau et possédant une adresse unique sur ledit deuxième réseau, d'un premier message représentatif d'une information confidentielle,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif de ladite information confidentielle, et

- une opération de transmission, sur le premier support de transmission, en provenance du premier terminal et à destination du deuxième terminal, d'un message représentatif de l'information confidentielle.

Dans chacun des aspects de la présente invention, l'utilisateur, d'une part, et la transaction, d'autre part, sont donc authentifiés car la transmission de l'information confidentielle, à l'initiative de l'utilisateur, prouve son identité par la réception de cette information confidentielle. De plus, l'engagement de l'utilisateur dans les deux communications, prouve l'utilisation des deux terminaux, simultanément, par le même utilisateur.

Lorsque l'un des réseaux utilisés est un réseau de communication mobile, la mise en oeuvre de l'invention est entièrement nomade, c'est-à-dire qu'elle peut être appliquée n'importe où, par l'utilisateur du réseau de communication mobile.

En outre, l'invention peut être mise en oeuvre sur n'importe quels terminaux et est indépendante du matériel utilisé. Elle ne nécessite aucune adaptation des terminaux actuels, ni modification, ni ajout de périphériques.

La simplicité de mise en oeuvre de la présente invention rend les tâches d'authentification, de virement, de paiement, intuitives, et elle ne nécessite aucun apprentissage.

On observe aussi que l'information confidentielle peut être un mot de passe ou un certificat de transaction.

Selon des caractéristiques particulières de chacun des aspects de la présente invention exposés ci-dessus :

- l'information confidentielle est représentative d'un nombre pseudo-aléatoire,

- l'information confidentielle est représentative d'un numéro de session attribué à une session,

- l'information confidentielle est représentative de l'identifiant de l'utilisateur,

- l'information confidentielle est représentative d'un ou plusieurs numéros de compte bancaire et/ou de carte,

- l'information confidentielle est représentative de l'heure et la date de ladite opération d'ouverture de session, et/ou

- l'information confidentielle est modifiée à chacune des sessions.

Grâce à chacune de ces dispositions, l'information confidentielle est renouvelée à chaque session et son usage est limité à une seule session de communication.

Selon des caractéristiques particulières de chacun des aspects de l'invention exposés ci-dessus:

- au cours de l'opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de communication, on reçoit, en outre, un montant de transaction, et/ou

- au cours de l'opération de transmission d'un message confidentiel représentatif de l'information confidentielle, on transmet, en outre, un montant de transaction.

Grâce à chacune de ces dispositions, l'invention permet des transactions mettant en oeuvre des montants financiers, telles que des achats, des réservations, des échanges, des emprunts, des mises en gages, des cautions ...

Selon un neuvième aspect, la présente invention vise un procédé de transmission d'information sur un premier support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un premier terminal, d'un premier message représentatif :
  . d'un montant d'une transaction envisagée,
  . d'un identifiant d'un débiteur,
- une opération de transmission, sur un deuxième support de communication, à un serveur bancaire, d'un deuxième message représentatif :
  . dudit montant,
  . d'un identifiant dudit débiteur
  . d'une demande d'autorisation de débit,
- une opération de réception ou non de la part dudit serveur bancaire, d'un troisième message représentatif d'une autorisation de débit,
- lorsque l'autorisation est accordée, une opération de transmission, à un deuxième terminal possédant une adresse unique sur un deuxième réseau de communication, d'un quatrième message représentatif d'une information confidentielle,
- une opération de réception, de la part dudit premier terminal, d'un cinquième message représentatif de ladite information confidentielle,
- une opération de vérification de correspondance entre le message confidentielle et l'information confidentielle.

Ce neuvième aspect de la présente invention présente les mêmes avantages que les premier et deuxième aspects. Ces avantages ne sont donc pas rappelés ici.

Selon des caractéristiques particulières de chaque aspect de l'invention, après l'opération de vérification de correspondance, en cas de correspondance, le procédé visé par la présente invention, tel que succinctement exposé ci-dessus comporte une opération d'incrémentation d'un compte au débit dudit débiteur.

Grâce à ces dispositions, une facture correspondant à chaque montant de transaction effectué par le débiteur, peut lui être envoyée.

Selon d'autres caractéristiques particulières de chacun des procédés visés par les différents aspects de la présente invention, ce procédé comporte, après l'opération de réception du premier message, une opération de lecture, dans une base de donnée, de l'adresse unique du deuxième terminal sur le deuxième réseau.

Grâce à ces dispositions, le débiteur n'a pas a fournir cette adresse, d'une part, et cette adresse est certifiée, d'autre part.

Selon d'autres caractéristiques particulières de chacun des procédés visés par les différents aspects de la présente invention, ce procédé comporte, après l'opération de réception du premier message, une opération de lecture, dans une base de donnée, d'un identificateur dudit serveur bancaire.

Grâce à ces dispositions, le débiteur n'a pas a fournir cet identificateur, ni une carte bancaire, d'une part, et cet identificateur peut être préliminairement vérifié, d'autre part.

Selon un dixième aspect, la présente invention vise un procédé de transmission d'information sur un premier support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un premier terminal, d'un premier message représentatif :
  . d'un montant d'une transaction envisagée,
  . d'un identifiant d'un débiteur,
- une opération d'autorisation, ou non, de débit d'un compte bancaire,
- lorsque l'autorisation est accordée, une opération de transmission, à un deuxième terminal possédant une adresse unique sur un deuxième réseau de communication, d'un deuxième message représentatif de l'information confidentielle,
- une opération de réception, de la part dudit premier terminal, d'un troisième message représentatif de ladite information confidentielle,
- une opération de vérification de correspondance entre le message confidentielle et l'information confidentielle et
- dans le cas où la correspondance est vérifiée, une opération de débit dudit montant sur ledit compte bancaire.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, celui-ci comporte une opération de saisie

manuelle, au cours de laquelle l'utilisateur saisit un message confidentiel représentatif de l'information confidentielle.

Grâce à ces dispositions, l'engagement de l'utilisateur est garantie par la saisie manuelle qu'il effectue.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, celui-ci comporte une opération de sélection de transmission, au cours de laquelle, en fonction de critères prédéterminés, les transmissions sont classées en deux groupes, l'un concernant les transmission dites « à sécuriser » et l'autres les transmissions dites « normales », les transmissions normales ne donnant pas lieu à plus d'une opération de transmission sur un support de communication.

Grâce à ces dispositions, le procédé visé par la présente invention n'est mis en oeuvre que pour une partie des transmissions, en fonctions de critères prédéterminés.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, au cours de ladite opération de sélection, on met en oeuvre un montant limite de transaction, les transmissions dites « à sécuriser » étant celles auxquelles sont associées les montants de transaction supérieurs audit montant limite.

Grâce à ces dispositions, le critère de sélection des transmissions qui sont sécurisées par la mise en oeuvre de la présente invention sont celles qui concernent des montants de transaction supérieurs au montant limite.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, celui-ci comporte une opération de transmission d'une adresse unique sur l'un desdits réseaux.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, au cours de ladite opération de transmission d'une adresse unique, on transmet un certificat contenant une information représentative du ladite adresse unique.

Grâce à chacune de ces dispositions, c'est l'utilisateur lui-même ou, respectivement, son ordinateur, qui, de manière cryptée ou non, transmet sur l'un des réseaux une adresse unique dont il dispose sur un des réseaux utilisés.

Selon des caractéristiques particulières de chacun des aspects du procédé visé par la présente invention, ledit certificat répond à un protocole de sécurisation de paiement et comporte une information représentative de ladite adresse unique.

Grâce à ces dispositions, l'adresse unique transmise avec le certificat est protégé par le protocole de sécurisation de paiement.

La présente invention vise aussi une mémoire, amovible ou non, qui conserve des instructions d'un programme susceptible d'être exécuté par un processeur et adapté à mettre en oeuvre le procédé de transmission tel que succinctement exposé ci-dessus.

La présente invention vise, en outre, un serveur informatique, caractérisé en ce qu'il est adapté à mettre en œuvre le procédé de transmission tel que succinctement exposé ci-dessus.

Ce dixième aspect, ce serveur et cette mémoire présentant les mêmes caractéristiques particulières et les mêmes avantages que les neuf premiers aspects de la présente invention, exposés ci-dessus, ceux-ci ne sont pas rappelés ici.

D'autres avantages, buts et caractéristiques de l'invention ressortiront de la description qui va suivre, faite en regard des dessins annexés dans lesquels :

- la figure 1 est un schéma de principe du procédé de la présente invention ;

- la figure 2 représente un schéma particulier de mise en oeuvre de la présente invention ;

- la figure 3 représente une architecture système capable de supporter la mise en oeuvre de la présente invention ;

- la figure 4 représente une succession d'opérations génériques mises en oeuvre par les éléments illustrés en figures 2 et 3 ;

- la figure 5 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention à l'authentification; et

- la figure 6 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention à la certification de messages ;

- la figure 7 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement électronique en ligne, dans le cas d'un service sans abonnement ;

- la figure 8 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement électronique en ligne, dans le cas d'un service avec abonnement ;

- la figure 9 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une application de la présente invention au paiement avec un terminal de paiement électronique connu ;

- la figure 10 représente une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans le cadre d'une autre application de la présente invention au paiement électronique en ligne avec un tiers de confiance, dans le cas d'un service sans abonnement ;

- la figure 11 représente, schématiquement, des communications de messages mises en oeuvre dans une application de la présente invention en combinaison avec un protocole de paiement connu sous le nom de « SET » (acronyme de « Secure Electronic Transaction » pour transaction électronique sécurisée)

- la figure 12 représente, schématiquement, des communications de messages mises en oeuvre dans une application de la présente invention en combinaison avec un protocole de paiement connu de l'homme du métier sous le nom de GlobeId (marque déposée) ou Kleline (marque déposée) ; et

- la figure 13 représente, schématiquement, des communications de messages mises en oeuvre dans une application de la présente invention en combinaison avec un protocole de communication sécurisé connu sous le nom de « SSL » (acronyme de « Secure Socket Level » pour niveau de sécurité (*??*).

En **figure 1** sont représentés :

- un premier réseau 10,
- un premier terminal de premier réseau 11,
- un deuxième terminal de réseau, aussi appelé par la suite " serveur de données et de messages " 40,

- un deuxième réseau 20,
- un troisième terminal de deuxième réseau 21, et
- un serveur d'information 30.

Selon l'invention, l'utilisateur du premier terminal 11 est identifié par son adresse unique sur le deuxième réseau 20.

Celui-ci est préférentiellement sécurisé, c'est-à-dire que chaque adresse y est certifiée par un tiers de confiance, et, en outre, l'information transmise est confidentielle. Le tiers considéré est préférentiellement un opérateur de téléphonie, ou, plus généralement, tout organisme qui dispose d'une base de données d'utilisateur d'un terminal à adresse unique.

Le terminal de premier réseau 11 peut être, par exemple, un téléphone, un terminal informatique, un télécopieur, un terminal télématique, un téléviseur équipé d'un boîtier adapté à recevoir et à émettre des données informatiques (boîtier communément appelé un décodeur de télévision), un terminal de paiement électronique (figure 2).

Le terminal de deuxième réseau 21 peut être, par exemple, un téléphone, un télécopieur, un terminal télématique, un décodeur de télévision, un téléphone mobile ou un récepteur de messages («pageur») ou un assistant personnel numérique (communément appelé «PDA»).

Dans un premier mode de réalisation de la présente invention, dans un premier temps, l'utilisateur utilise le terminal 11 de premier réseau 10 pour entrer en communication avec le serveur d'information 30. Il ouvre ainsi une session de communication entre le terminal 11 et le deuxième terminal de réseau 40. Ensuite, le serveur d'information 30 fournit une information confidentielle à l'utilisateur, par l'intermédiaire :

- du serveur de données et de messages 40,
- du deuxième réseau 20, et
- du terminal de deuxième réseau 21.

Enfin, l'utilisateur reçoit l'information confidentielle au niveau du terminal du deuxième réseau 21 et effectue une saisie manuelle d'un message confidentiel, constitué ici de l'information confidentielle, pour le transmettre au serveur d'information 30, au cours de la même session, par l'intermédiaire :

- du terminal de premier réseau 11 et
- du premier réseau 10.

Le serveur de données et de messages 40 vérifie alors la correspondance du message confidentiel et de l'information confidentielle, c'est-à-dire si le message confidentiel est représentatif de l'information confidentielle, et, en cas de correspondance, il donne l'accès à des services particuliers, payants ou confidentiels.

L'utilisateur, d'une part, et la transaction, d'autre part, sont donc authentifiés car la saisie manuelle prouve l'identité de l'utilisateur qui reçoit l'information confidentielle ainsi que l'utilisation des deux terminaux simultanément par le même utilisateur.

En **figure 2** sont représentés :

- un premier terminal, dit «utilisateur» 100 relié à un premier support de communication 101 faisant partie d'un réseau de communication ;
- un serveur d'information 103, relié au premier support d'information 101 ;
- un serveur de données 105, relié par une ligne de télécommunication 106 et/ ou une ligne informatique 106 au serveur d'information 103 ;
- un serveur de messages 109, reliée par un deuxième support de communication 110 à un récepteur 111 et par un troisième support de communication 113, au serveur de données 105 ; et
- une base de données d'abonnés 107 reliée au serveur de message 109 et au serveur de données 105.

Dans le mode de réalisation décrit et représenté ici, le terminal utilisateur 100 est un ordinateur personnel (communément appelé " PC ") ou un ordinateur de réseau (communément appelé " NC "), ou encore un Minitel (marque déposée) qui comporte un modem relié à un réseau de télécommunication filaire, comme par exemple le réseau téléphonique commuté. Le premier support de communication 101 est alors un canal de ce réseau de télécommunication. Le terminal utilisateur 100 met en oeuvre un logiciel de communication de type connu, qui lui permet de communiquer à distance avec le serveur d'information 103, par l'intermédiaire du support de communication.

Le serveur d'information 103, relié au premier support d'information 101 est un serveur informatique de type connu, qui est ici adapté à mettre en oeuvre un logiciel spécifique, conforme à l'invention (illustré en l'une des figures 4 à 13).

Le serveur de données 105 est un serveur informatique de type connu qui fonctionne comme il est indiqué ci-dessous, en relation avec le serveur d'information 103, par l'intermédiaire de la ligne 106, elle aussi de type connu.

Le serveur de messages 109 est un système informatique de type connu qui gère un ou des réseaux de communication de types connus, un canal de l'un de ces réseaux constituant un deuxième support de communication. Un canal spécialisé fournit le troisième support 113 pour la communication entre le serveur d'information 103 et le serveur de messages 109.

La base de données d'abonnés 107 est un registre de mémoire de type connu.

On observe ici que la base de données d'abonnés 107 peut être reliée directement à plusieurs systèmes informatiques :

- à celui du fournisseur de service dans le cas d'un réseau externe à une entreprise, en particulier dans certains cas de mise en oeuvre de la présente invention avec un abonnement préalable de l'utilisateur au service,

- dans l'entreprise, dans le cas où le réseau est interne à l'entreprise,

- à celui d'une banque ou d'un tiers de confiance, en particulier dans le cas d'utilisation de l'invention sans abonnement.

Enfin, dans certains cas, la base de données n'est pas nécessaire, l'adresse unique sur le deuxième réseau étant fournie, sur le premier réseau, soit par un certificat de protocole de paiement stocké sur le poste (ou « ordinateur ») client, soit par l'utilisateur, lui-même.

Le deuxième support de communication 110 est un réseau de communication de type connu. Sur ce deuxième réseau, chaque récepteur possède une adresse unique qui est certifiée au moment de l'attribution de l'adresse du récepteur 111.

Le récepteur 111 est, dans le mode de réalisation décrit et représenté ici, un téléphone portable (communément appelé «mobile») ou un récepteur de message (communément appelé " pageur "), un télécopieur ou un téléphone fixe ou un terminal équipé d'un modem. Il est adapté à recevoir un message confidentiel et

à le mettre à disposition de l'utilisateur, par exemple par affichage sur écran, émission vocale ou impression sur papier. En variante, les serveurs d'information 103 et le serveur de messages 109 sont confondus.

On observe ici que :

- dans le cas où le récepteur 111 ne sert à l'utilisateur qu'à recevoir une information confidentielle sans émettre le message confidentiel, il n'est pas nécessaire qu'il permette l'émission sur le réseau 110,

- en revanche, lorsque, conformément à certaines variantes de la présente invention, le récepteur 111 sert d'une part à recevoir l'information confidentielle et d'autre part à émettre le message confidentiel, il est nécessaire qu'il permette l'émission sur le réseau 110.

En **figure 3**, on observe, dans une architecture matérielle et logicielle permettant la mise en oeuvre de la présente invention :

- un terminal informatique 301,
- un réseau informatique 302,
- un serveur d'information 103,
- un réseau local 304,
- un serveur de données 105,
- une base de données 107,
- un serveur de messages 109,
- un réseau 308,
- un moyen de diffusion 309,
- un réseau de radiotéléphonie 310,
- un réseau de téléphonie cellulaire 311,
- un récepteur de messages alphanumériques 312 (appelé " pageur "),
- un téléphone mobile 313,
- un réseau commuté 314, et
- un téléphone ou télécopieur 315.

Le terminal informatique 301 est, par exemple un micro-ordinateur connu sous le nom de «PC». Il comporte un modem permettant la communication en émission et en réception, avec le réseau informatique 302. Le réseau informatique 302 est ici le réseau informatique mondial connu sous le nom d'«internet». Le

serveur d'information 103 est de type connu pour la mise en oeuvre de sites de fournisseurs de services sur le réseau 302.

Le réseau local 304 est de type connu. C'est un réseau d'entreprise, par exemple du type LAN Manager (marque déposée) Netware (marque déposée de la société NOVELL, ce nom étant aussi une marque déposée).

Le serveur de données 105 et le serveur de message 109 sont de types connus. La base de données 107 est de type connu.

Le réseau 308 est de type connu, par exemple de type Réseau Numérique à Intégration de Service (« RNIS »).

Le moyen de diffusion 309 est un émetteur hertzien, de type connu pour la mise en oeuvre du réseau de communication mobile 310. Il est, par exemple cellulaire ou par satellite.

Dans le mode de réalisation décrit et représenté en figure 3, au moins l'un des trois réseaux de communication suivants est utilisé :

- le réseau de radiotéléphonie 310 qui ne permet que la communication dans le sens de la diffusion depuis un émetteur vers des récepteurs de messages alphanumériques comme le récepteur 312, sans que ceux-ci ne puissent émettre de signaux à distance,

- un réseau de téléphonie mobile 311, permettant la communication en particulier avec des téléphones mobiles, comme le téléphone 313, et

- un réseau commuté 314 permettant ici la communication avec un téléphone fixe ou un télécopieur fixe 315.

Ces trois réseaux fonctionnent par abonnement, avec certification de l'identité de l'abonné. Sur chacun de ces réseaux, le récepteur possède une adresse unique, c'est-à-dire que l'adresse qui lui est attribuée n'est pas attribuée à un autre récepteur (sauf dans certains cas d'abonnements groupés demandés par l'utilisateur). Cette adresse unique s'apparente à un numéro de téléphone et/ou à un numéro de carte SIM (acronyme de « Subscriber Identity Module » pour « module d'identité d'abonné »), module sécurisé d'identification du portable, par exemple, dans le cas d'un réseau de télécommunication mobile connu sous le nom de « GSM » (acronyme de « Global System for Mobile » pour « système globale pour mobiles »).

On observe ici que les appareils destinés à fonctionner sur le réseau GSM utilisent une carte à microprocesseur. Cette carte fournit aux modes particuliers de l'invention qui la mettent en œuvre l'avantage d'une double sécurité.

Dans le cas illustré en figure 3, c'est préférentiellement le même utilisateur qui met en oeuvre le terminal informatique 301, d'une part, et le récepteur alphanumérique 312, le téléphone mobile 313, le télécopieur fixe ou le téléphone fixe, d'autre part.

Les figures 4 à 9 qui illustrent différentes applications de la présente invention, utilisent le même formalisme : sur chacune de ces figures, les opérations sont représentées de haut en bas, dans l'ordre de leur succession chronologique. Sur ces figures, sont représentées :

- sur la colonne verticale la plus à gauche et sous forme de rectangles, les opérations effectuées par l'utilisateur, en mettant en oeuvre soit le terminal relié au premier support de communication («terminal A») soit le terminal relié au deuxième support de communication («terminal B»), le terminal utilisé étant inscrit dans un losange auquel le rectangle représentant l'opération considérée se superpose ;

- sur une colonne centrale, des transmissions d'information successives sur l'un ou l'autre support de communication (« A » pour le réseau informatique 302 ou « B » pour le réseau de télécommunication les réseaux 308, 310, 311 et/ou 314), sous forme de flèches dont le sens correspond au sens de communication, c'est-à-dire que le sens de gauche à droite, correspond au sens utilisateur vers serveur et que le sens de droite à gauche correspond au sens serveur vers utilisateur.

On observe ici que pour chaque transmission d'information, plusieurs signaux peuvent être échangés entre les systèmes électroniques mis en oeuvre (synchronisation, sélection de protocole de communication, information, redondances, acquittement de transmission, retransmission en cas d'erreur de transmission, ...). Dans ces flèches, le serveur «A» correspond au premier réseau et le serveur «B» au deuxième réseau ;

- sur une colonne verticale plus à droite que les deux précédentes (la plus à droite en figures 4 à 6 et 9), sous forme de rectangles, les opérations effectuées par le serveur de données 105 ; et

- en figures 7, 8 et 10, sur une colonne verticale située la plus à droite, un serveur mis en communication avec le serveur de données 105.

En **figure 4**, on observe une succession d'opérations mises en oeuvre dans certaines applications de l'invention, par les éléments illustrés en figures 2 et 3 :

- au cours d'une opération 200, l'utilisateur du terminal utilisateur 101 entre en communication avec le serveur d'information 103, par l'intermédiaire du premier support de communication. Au cours de cette opération 200, il fournit un identifiant unique (par exemple un numéro d'abonné, un nom ou une adresse physique) ;

- au cours de l'opération 201, le serveur d'information 103 attribue un numéro de session unique dès la connexion du terminal «utilisateur» 100 au serveur d'information 103. Au cours de cette opération 201, le serveur d'information 103 transmet l'identifiant au serveur de données 105 ;

- au cours de l'opération 202, le serveur de données 105 calcule une information confidentielle aussi appelée par la suite «secret», au serveur de messages 109. A cet effet, le serveur de données 105 calcule le secret comme étant une représentation d'une fonction algorithmique utilisant un invariant (c'est-à-dire une valeur qui ne varie pas d'une session à l'autre, comme l'identifiant, par exemple), un variant (c'est-à-dire une valeur qui varie à chaque sessions), pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (c'est-à-dire d'une valeur d'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle (ou «secret») irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 202, le lecteur pourra se référer à des livres d'algorithmes de sécurité bien connus, et en particulier aux descriptions des fonctions connues sous les noms de «hashing», «Message Digest», et «SHA» ;

- l'opération 203 prend plusieurs formes différentes selon que l'identifiant est déjà dans la base de données ou non : dans l'affirmative, l'adresse unique y est lue, dans la négative, il est fait appel à un tiers de confiance, qui est, ici, l'opérateur du deuxième réseau ou tout autre organisme habilité à jouer le rôle de tiers de confiance ;

- au cours de l'opération 204, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 203 ;

- au cours de l'opération 204, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle transmise au cours de l'opération 203 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 207, l'information confidentielle, aussi appelée ici «secret» est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 208, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle ou «secret»), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 205, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 210, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 202, ou non ;

- lorsque le résultat du test 210 est positif, le serveur de données 105 donne à l'utilisateur l'accès aux ressources protégées ;

- lorsque le résultat du test 210 est négatif, le serveur de données 105 transmet, à l'utilisateur, un message d'erreur, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et l'accès aux ressources protégées est refusé à l'utilisateur.

Enfin, la suite de la session ouverte sur le premier support de communication est de type connu, mais, grâce à la mise en œuvre de la présente invention, l'utilisateur est authentifié de manière forte.

On observe ici que, même si le secret venait à être connu, du fait que ce secret correspond au numéro de session unique attribué dynamiquement par le serveur d'information 103 et du fait que la session reste ouverte (mode connecté)

jusqu'à l'envoi du secret, ce secret ne pourrait être utilisé pour réaliser des opérations frauduleuses. En effet, toute nouvelle session ouverte se verrait alors attribuer un autre secret.

En **figure 5**, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention à l'authentification, pour accès à des données protégées :

- au cours d'une opération 500, l'utilisateur du terminal utilisateur 101 entre en communication avec le serveur d'information 103, par l'intermédiaire du premier support de communication. Au cours de cette opération 500, il fournit un identifiant unique (par exemple un numéro d'abonné, un nom, ou une adresse physique) ;

- au cours de l'opération 501, le serveur d'information 103 attribue un numéro de session unique dès la connexion du terminal utilisateur au serveur d'information 103. Au cours de cette opération 501, le serveur d'information 103 transmet l'identifiant au serveur de données 105 ;

- au cours de l'opération 502, le serveur de données 105 calcule une information confidentielle aussi appelée par la suite «mot de passe jetable», au serveur de messages 109. A cet effet, le serveur de données 105 calcule l'information confidentielle à partir d'un invariant (l'identifiant, par exemple), d'un variant pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 502, le lecteur pourra se référer aux livres mentionnés plus haut ;

- au cours de l'opération 504, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 503 ;

- au cours de l'opération 505, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle aussi appelée ici «mot de passe jetable», au cours de l'opération 503 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 507, l'information confidentielle, aussi appelée ici «mot de passe jetable» est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 508, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle, ou «mot de passe jetable»), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 509, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 510, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 503, ou non ;

- lorsque le résultat du test 510 est positif, le serveur de données 105 valide l'accès à l'information protégée ;

- lorsque le résultat du test 510 est négatif, le serveur de données 105 transmet un message d'erreur et d'invalidation d'accès, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et l'accès à l'information protégée est refusé.

Enfin, la fin de la session est de type connu.

En **figure 6**, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention à la certification de message :

- à la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103,

- au cours de l'opération 601, le serveur d'information 103 attribue un numéro de session unique ;

- au cours d'une opération 600, l'utilisateur du terminal «utilisateur» 100 initie, sur le premier support de communication, une procédure de transaction (par exemple virement de compte à compte, commande ou ordre boursier) (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 603, le serveur de données 105 calcule une information confidentielle aussi appelée, par la suite, «certificat de message» à

partir d'un invariant (l'identifiant, par exemple), d'un variant pour éviter les répétitions (numéro de session, par exemple) et d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps. Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 603, le lecteur pourra se référer aux livres mentionnés plus haut ;

- au cours de l'opération 604, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis, par le serveur d'information 103, au serveur de message 109, au cours de l'opération 603 ;

- au cours de l'opération 605, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle aussi appelée ici «certificat de message», transmis au cours de l'opération 603 au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 607, l'information confidentielle, aussi appelée ici «certificat de message» est fournie à l'utilisateur, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée ;

- au cours de l'opération 608, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel représentatif de l'information confidentielle (par exemple identique à cette information confidentielle, ou «certificat de message»), par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 609, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 610, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 603, ou non ;

- lorsque le résultat du test 610 est positif, le serveur de données 105 valide la transaction effectuée, puis reprend ;

- lorsque le résultat du test 610 est négatif, le serveur de données 105 transmet un message d'erreur et d'invalidation de transaction, en précisant

éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et ne réalise pas la transaction.

Enfin, la fin de la session est de type connu.

Selon une variante non représentée :

- au cours de l'opération 603, le «certificat de message» est aussi déterminé, par le serveur de données 105, à partir d'un montant d'un virement et/ou d'un numéro de compte bancaire émetteur et/ou d'un numéro de compte bancaire récepteur,

- au cours de l'opération 605, le serveur de messages 109 transmet, par l'intermédiaire du réseau 110, l'information confidentielle et le montant du virement, en clair et, plus généralement, une information représentative de la transaction effectuée (produit ou service acquis et quantité concernée) ; et

- au cours de l'opération 607, l'information confidentielle ainsi que le montant sont fournis à l'utilisateur qui vérifie l'intégrité du montant du virement en cours.

En **figure 7**, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement électronique en ligne, dans le cas d'un service sans abonnement :

- à la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103,

- au cours de l'opération 700, le serveur d'information 103 attribue un numéro de session unique secret ;

- au cours d'une opération 701, le serveur d'information 103 reçoit de la part du terminal utilisateur 100, un identifiant ;

- au cours d'une opération 702, l'utilisateur du terminal utilisateur 101 choisit un bien ou un service qu'il souhaite acheter, puis initie une procédure de paiement (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 703, le serveur de données 105 reçoit la demande de paiement de la part du terminal utilisateur 100 ;

- au cours de l'opération 704, l'utilisateur fournit au serveur d'information 103 de l'information confidentielle concernant sa carte de paiement ;

- au cours d'une opération 705, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant

transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 701 ;

- au cours d'une opération 707, le serveur de données 105 effectue une demande d'autorisation bancaire au serveur 706 d'une banque où l'utilisateur dispose du compte auquel est rattaché la carte de paiement concernée par l'opération 704. Le serveur de données 105 fournit le montant de la transaction envisagée au serveur bancaire 706. Le serveur d'information 103 reçoit, en retour, de la part du serveur bancaire 706, une autorisation de paiement, selon des modalités bancaires de type connues qui dépendent, en particulier, des conventions passées entre la banque et le client considéré et de l'éventuelle autorisation de découvert sur ledit compte (voir le protocole connu de l'homme du métier sous le nom de « CBSA » pour « Carte Bancaire Système Autorisation ») ;

- au cours d'une opération 708, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite «certificat de transaction» à partir :

. d'un invariant (l'identifiant, par exemple),

. d'un variant pour éviter les répétitions (numéro de session, par exemple),

. du montant de la transaction et

. d'un marqueur temporel (l'horloge) afin de borner l'utilisation d'un secret dans le temps.

Préférentiellement, il met en oeuvre une fonction de calcul d'information confidentielle irréversible, c'est-à-dire dont on ne peut retrouver l'information d'entrée lorsque l'on connaît celle de sortie. Pour la mise en oeuvre de l'opération 708, le lecteur pourra se référer aux livres mentionnés plus haut. Au cours de cette opération 708, le certificat de transaction et le montant de la transaction envisagée sont diffusés, par l'intermédiaire du réseau 110, au récepteur 111 qui possède ladite adresse unique ;

- au cours de l'opération 709, l'information confidentielle, aussi appelée ici «certificat de transaction» est mise à disposition de l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée, ce qui permet le contrôle, par l'utilisateur, de l'intégrité de la transaction qu'il réalise ;

- au cours de l'opération 710, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à (ou, en variante, représentatif de) l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 711, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 712, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 708, ou non ;

- lorsque le résultat du test 712 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant effectivement réalisé entre les organismes bancaires selon des techniques connues, puis reprend le fonctionnement de présentation d'offres commerciales ;

- lorsque le résultat du test 712 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Enfin, la fin de la session est de type connu.

En variante du mode de réalisation illustré en figure 7, l'opération 707 est effectuée après toutes les autres opérations, mais avant la fin de session.

En **figure 8**, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement électronique en ligne, dans le cas d'un service avec abonnement :

- à la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103,

- au cours de l'opération 800, le serveur d'information 103 attribue un numéro de session unique secret ;

- au cours d'une opération 801, le serveur d'information 103 reçoit de la part du terminal utilisateur 100, un identifiant ;

- au cours d'une opération 802, l'utilisateur du terminal utilisateur 101 choisit un bien ou un service dont il souhaite avoir le bénéfice, puis initie une procédure de paiement (voir ci-dessus en regard de la figure 4) ;

- au cours de l'opération 803, le serveur de données 105 reçoit la demande de paiement de la part du terminal utilisateur 100 ;

- au cours de l'opération 805, le serveur de données 105 effectue, préférentiellement de manière sécurisée, une demande d'autorisation bancaire au serveur 706 d'une banque où l'utilisateur dispose du compte auquel est rattaché la carte de paiement concernée par l'opération 804. Il fournit le montant de la transaction envisagée au serveur bancaire 806 ainsi que des données concernant la carte de paiement, ces données étant conservées par le serveur d'information 103 à compter de l'abonnement de l'utilisateur au service considéré. Le serveur d'information 103 reçoit, en retour, de la part du serveur de banque 806, une autorisation de paiement, selon des modalités bancaires qui dépendent du montant disponible sur le compte bancaire considéré et de l'éventuelle autorisation de découvert sur ledit compte ;

- au cours d'une opération 807, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 801 ;

- au cours d'une opération 808, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite, «certificat de transaction» (voir figure 7) ;

- au cours de l'opération 809, l'information confidentielle, aussi appelée ici «certificat de transaction» est fournie à l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale ou télécopiée, ce qui permet le contrôle de l'intégrité de la transaction par l'utilisateur ;

- au cours de l'opération 810, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à, ou, en variante, représentatif de, l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du terminal utilisateur 100 ;

- au cours de l'opération 811, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 812, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 808, ou non ;

- lorsque le résultat du test 812 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant ensuite effectivement réalisé entre les organismes bancaires selon des techniques connues, puis reprend le fonctionnement de présentation d'offres commerciales ;

- lorsque le résultat du test 812 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Enfin, la fin de la session est de type connu.

En variante du mode de réalisation illustré en figure 8, l'opération 805 est effectuée après toutes les autres opérations, mais avant la fin de session.

En **figure 9**, on observe une succession d'opérations mises en oeuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement avec un terminal de paiement électronique :

- au cours d'une opération 915, l'utilisateur introduit sa carte de paiement dans un terminal de paiement électronique («TPE») qui constitue le terminal dit «utilisateur» ;

- au cours d'une opération 916, le commerçant saisit le montant de la transaction sur ledit TPE ;

- au cours d'une opération 900, une ouverture de session est effectuée entre le TPE 100, et le serveur d'information 103 et un numéro de session unique et secret est attribué par le serveur de communication 103 ;

- au cours d'une opération 901, le serveur d'information 103 reçoit de la part du TPE 100, des informations portées par la carte de paiement ainsi que le montant de la transaction en cours, et le serveur d'information transmet une demande de l'identifiant du consommateur auprès de l'organisme bancaire 906 et reçoit cet identifiant en retour ;

- au cours d'une opération 907, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis au cours de l'opération 901 ;

- au cours d'une opération 908, le serveur d'information 103 calcule une information confidentielle aussi appelée, par la suite, «certificat de transaction» (voir figure 7) ;

- au cours de l'opération 909, l'information confidentielle, aussi appelée ici «certificat de transaction» est fournie à l'utilisateur, conjointement au montant de la transaction, en clair, soit en étant affichée sur l'afficheur du récepteur 111, soit en étant donnée de manière vocale, ce qui permet le contrôle de l'intégrité de la transaction par l'utilisateur ;

- au cours de l'opération 910, l'utilisateur fournit au serveur d'information 103, qui, lui-même, le retransmet au serveur de données 105, un message confidentiel identique à, ou, en variante, représentatif de, l'information confidentielle constituée par le certificat de transaction, par l'intermédiaire du clavier du TPE 100 ;

- au cours de l'opération 911, le serveur d'information 103 reçoit ce message confidentiel ;

- au cours du test 912, le serveur de données 105 détermine si ce message confidentiel est représentatif de l'information confidentielle générée par le serveur de données 105, au cours de l'opération 908, ou non ;

- lorsque le résultat du test 912 est positif, le serveur de données 105 valide le paiement effectué, ce paiement étant ensuite effectivement réalisé entre les organismes bancaires selon des techniques connues ;

- lorsque le résultat du test 912 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Une variante de l'opération 916 est la saisie par l'utilisateur de son code personnel aussi appelé «PIN»(acronyme de « Personal Identification Number » pour « numéro d'identification personnel »), avant le lancement de l'opération 900.

Enfin, la fin de la session est de type connu et le client récupère sa carte de paiement ainsi qu'un ticket imprimé portant le montant du paiement effectué.

En **figure 10**, on observe une succession d'opérations mises en œuvre par les éléments illustrés en figures 2 et 3, dans une application de l'invention au paiement électronique en ligne, utilisant un tiers de confiance, dans le cas d'un service sans abonnement, application différente de celle illustrée en figure 7.

Dans cette application, le serveur de données 105 est situé préférentiellement avec le serveur de messages 109, et fait partie, avec celui-ci, du tiers de confiance (aussi appelé tiers certificateur). A titre d'exemple, ces deux serveurs 105 et 109 se trouvent chez l'opérateur de télécommunication.

Dans cette applications, les opérations mises en œuvre se succèdent de la manière suivante.

A la suite d'une opération d'ouverture de session, non représentée, entre le terminal utilisateur 100 et le serveur d'information 103, au cours d'une opération 1000, le serveur d'information 103 attribue un numéro de session unique secret. Au cours d'une opération 1001, l'utilisateur du terminal utilisateur 101 choisit un bien ou un service qu'il souhaite acheter, puis initie une procédure de paiement, en coopération avec le serveur d'information 103.

Le serveur d'information 103 reçoit alors, au cours d'une opération 1032, une demande de paiement et, en particulier, un montant de la transaction envisagée.

Au cours d'une opération 1003, l'utilisateur du terminal utilisateur 101 fournit un identifiant et, au cours d'une opération 1004, le serveur d'information 103 reçoit cet identifiant de la part du terminal utilisateur 100.

Au cours d'une l'opération 1005, le serveur d'information 103 transmet une demande de paiement ainsi que l'identifiant de l'utilisateur et le montant de la transaction envisagée, au serveur de données 105, par l'intermédiaire de la ligne de télécommunication 106. Au cours d'un test 1006, le serveur de données 105 détermine si le montant de la transaction envisagé est supérieur à un montant prédéterminé.

Lorsque le résultat du test 1006 est négatif, une opération 1008 est effectuée (voir ci-dessous).

Lorsque le résultat du test 1006 est positif, le serveur de données 105 recherche, au cours d'une opération 1007, dans sa base de données d'abonnés, le numéro de la carte bancaire correspondant à l'identificateur transmis et effectue une demande d'autorisation bancaire à un serveur d'une banque où l'utilisateur dispose du compte auquel est rattaché cette carte de paiement.

Au cours d'un test 1009, le serveur de la banque détermine, selon des règles connues en soit, si la transaction envisagée est autorisée, ou non. Lorsque le résultat du test 1009 est négatif, un refus est signifié à l'utilisateur, au cours d'une opération non représentée, par l'intermédiaire du serveur d'information 103 et du terminal utilisateur 101.

Lorsque le résultat du test 1009 est positif, le serveur de données 105 reçoit, au cours de l'opération 1008, de la part du serveur de banque, une autorisation de paiement, selon des modalités bancaires connues.

Au cours de l'opération 1008, l'adresse unique du récepteur 111 est déterminée : elle est représentative, dans la base de données 107, de l'identifiant transmis par le serveur d'information 103 au serveur de message 109, au cours de l'opération 1001.

Puis, les opérations 708 et suivantes exposées en regard de la figure 7, sont effectuées.

Cependant, dans le mode de réalisation illustré en figure 10, lorsque le résultat du test 712 est positif, le serveur de données 105 valide le paiement effectué, puis retourne un accord de paiement au serveur 103, accompagné de l'adresse de l'abonné du service téléphonique (A l'issue de la période de facturation téléphonique du tiers de confiance, ce paiement étant effectivement réalisé entre les organismes bancaires de l'acheteur et du tiers de confiance, selon des techniques connues. De même à l'issue d'une période de paiement, le tiers de confiance effectue la remise commerçant et prélève, éventuellement, des frais de service.), puis reprend le fonctionnement de présentation d'offres commerciales.

En revanche, lorsque le résultat du test 712 est négatif, le serveur de données 105 transmet à l'utilisateur un message d'erreur et d'invalidation du paiement, en précisant éventuellement une cause d'échec (trop de temps écoulé entre la transmission de l'information confidentielle et sa réception, ...) et le paiement n'est pas effectué.

Enfin, la fin de la session est de type connu.

En **figure 11**, on observe un schéma de système de paiement conforme à la présente invention et mettant en oeuvre les protocoles de paiement connus sous le nom de « SET » (acronyme de « Secure Electronic Transaction » pour « transaction électronique sécurisée »). Pour mieux connaître ce type de transaction, le lecteur se reportera à la version 1.0 des spécifications du protocole SET, publiée le 31 Mai 1997. Cette version est incorporée ici par référence.

Pour mémoire, on rappelle que les entreprises VISA (marque déposée) et MASTERCARD (marque déposée) se sont associées pour définir un standard commun de paiement par cartes bancaires à travers des réseaux ouverts : le protocole SET.

Les principaux objectifs de ce protocole SET sont les suivants :

- rendre facile et rapide le développement du commerce électronique,
- créer la confiance sur le réseau entre acheteur et vendeur au moyen d'un échange de certificats,
- séparer le réseau Internet du réseau bancaire,
- garantir l'intégrité et la confidentialité des transactions grâce au chiffrement des messages,
- assurer l'interopérabilité entre standard bancaire ouvert et solution non propriétaire,
- s'appuyer sur des normes déjà existantes.

Les principes et le fonctionnement du protocole SET s'appuient sur trois notions importantes :

- le Gestionnaire de Télépaiement (connu de l'homme du métier sous le nom de « Payment Gateway »), qui assure l'étanchéité entre le domaine Internet et le domaine bancaire,
- les certificats qui sont des clés publiques qui servent à authentifier les différents acteurs entrant dans la transaction (porteur-client, commerçant, Gestionnaire de Télépaiement),
- le tiers de confiance qui certifie les clés publiques qui deviennent alors des certificats.

L'ensemble du système SET repose sur l'utilisation de certificats. Le tiers de confiance certifie les clés publiques des porteurs-clients, des commerçants

et des Gestionnaires de Télépaiement. Le tiers de confiance fait, lui-même, l'objet d'une certification. On a ainsi un système en cascade, où un tiers de confiance d'un niveau supérieur certifie un tiers de confiance d'un niveau inférieur. Le système est hiérarchique et, au sommet, se trouve l'Autorité Suprême qui est connue de tous et qui n'a pas besoin de s'authentifier. L'intérêt d'une telle hiérarchie est de déléguer le travail de certification, tout en garantissant l'ensemble du système.

1) Pour son inscription, le client obtient sa clé en utilisant un logiciel spécifique qui sera intégré dans le navigateur, connu de l'homme du métier sous le nom de « browser » (ou « butineur »). Il entre son numéro de carte bancaire dans le programme. Celui-ci rend un fichier que le client doit renvoyer à l'une des entreprises VISA ou MASTERCARD, celle-ci renvoyant un certificat contenant une clé qui demeurera gravée dans le logiciel stocké sur le poste client.

2) Pour la transaction :

- le porteur consulte le catalogue sur le serveur et fait son choix. Le serveur commerçant envoie alors au client un bon de commande virtuel (Order Information « OI ») qui contient les informations sur le produit et le montant, ainsi que le certificat et la clé publique du commerçant et du Gestionnaire de Télépaiement ;

- le client envoie, au serveur commerçant, son certificat et sa clé publique. Donc, disposant de leur certificat réciproque, ils peuvent procéder à leur identification mutuelle ;

- le client crée ensuite un PI (acronyme de « Payment Information » pour « Information de Paiement »). Ce PI contient des informations relatives au système bancaire, qui sont destinées exclusivement au Gestionnaire de Télépaiement. Pour cette raison, le client chiffre le PI avec la clé publique du Gestionnaire de Télépaiement. Cette opération terminée, le client assemble le bon de commande virtuel OI et l'information de paiement PI, et signe le tout avec sa clé privée. Ce paquet est envoyé au serveur commerçant.

- le serveur commerçant est en mesure de vérifier la validité du paquet grâce à la clé publique du client. Il peut donc s'assurer que le client n'a pas modifié le bon de commande OI. Toutefois, il lui est impossible de lire d'information de paiement PI. Le serveur commerçant signe, à son tour, le paquet reçu et le transmet au Gestionnaire de Télépaiement. Le bon de commande émis par le serveur

commerçant et l'ordre de paiement émis par le porteur sont liés d'une manière indissociable au moyen de cette signature duale.

- le Gestionnaire de Télépaiement vérifie les certificats, la signature duale et la cohérence entre le bon de commande (OI) et l'ordre de paiement (PI). Il sert alors d'interface avec le monde traditionnel du paiement par carte.

- si les conditions habituelles de paiement par carte sont remplies, il confirme la transaction au serveur commerçant.

L'avantage de ce protocole est que, grâce aux certificats, le client et le serveur commerçant peuvent s'identifier mutuellement avant même d'effectuer la transaction.

Les inconvénients de ce protocoles sont que :

- la multiplication des tiers de confiance est lourde à gérer,

- la protection n'est que logicielle,

- les certificats sont stockés sur les machines des clients. Donc, en toute rigueur, l'authentification ne concerne pas le client mais son ordinateur.

En regard de la figure 11, on observe la mise en oeuvre de l'invention dans le cadre de la solution de paiement SET. Ce protocole met en oeuvre une relation tripartite, ordinateur du client 1101 - serveur commerçant 1102 - Gestionnaire de Télépaiement 1103. Chacune de ces entités reçoit des certificats SET générés par un gestionnaire de certification non représenté. A la date du dépôt de la présente demande de brevet, le protocole SET ne permet pas l'authentification de manière forte de l'acheteur, sauf à installer un lecteur de cartes à mémoire.

Dans un premier temps, un client initie l'achat en choisissant un bien ou un service sur un site commerçant d'un réseau informatique. Le client déclenche ensuite le paiement en validant l'achat (par exemple en cliquant sur une icône " validation achat ").

Ensuite, le client doit taper un mot de passe statique pour initialiser le paiement, en déchiffrant le certificat SET stocké sur son ordinateur.

Selon une variable non représentée, un mode opératoire consiste à ne pas utiliser de certificat (conformément au protocole SET fonctionnant en mode « 2 Kp »). Dans ce cas, aucun certificat n'est échangé et seule une authentification du client est nécessaire, conformément à la présente invention (ci-dessous).

Les échanges « ordinateur du client - serveur commerçant - Gestionnaire de Télépaiement » s'initient afin de déterminer les paramètres de communication (trames appelées « *PWakeUp* », « *PInitReq* » et « *PInitRes* » dans la spécification du protocole SET), les données contenues dans le certificat Client sont récupérées au niveau du Gestionnaire de Télépaiement (trame *Preq(PAN)*) qui les déchiffre et adresse une demande d'authentification du Client au serveur d'authentification 1104.

Ce serveur authentifie la transaction en calculant un code d'authentification de la transaction (« CAT ») et l'envoie, par l'intermédiaire d'un message court (connu de l'homme du métier sous le nom de « SMS », acronyme de « Short Message System » pour « Système de Messages Courts ») au client identifié par son numéro de téléphone mobile 1105 correspondant, dans la base de données abonnés, à l'identifiant déchiffré dans le certificat SET Client qui est reçu par le Gestionnaire de Télépaiement.

Selon une variante non représentée, le numéro de téléphone de l'abonné, sur le deuxième réseau, est inclus, chiffré, dans un champ du certificat client SET. Dans ce cas, il n'est pas nécessaire de disposer d'une base de données effectuant la correspondance entre le numéro de mobile de l'abonné et son identifiant. A la réception du certificat client sur le Gestionnaire de Télépaiement, celui-ci déchiffre le certificat et utilise directement le numéro du mobile contenu dans le certificat pour adresser le code d'authentification de la transaction du client. Ce principe de fonctionnement facilite l'interopérabilité entre les opérateurs de télécommunication et bancaires.

Le client reçoit alors un code d'authentification de transaction sous forme de message confidentiel, conformément à la présente invention. Il saisit ce message sur son ordinateur dans un champ d'authentification prévu à cet effet.

Le code d'authentification de transaction est alors envoyé soit par l'intermédiaire du serveur commerçant, directement au Gestionnaire de Télépaiement, soit le soumet au serveur d'authentification qui le valide et déclenche le paiement.

Selon une variante non représentée, le client reçoit sous forme de message court SMS le montant de la transaction en clair associé au Code d'identification de la transaction afin qu'il vérifie l'intégrité du montant de son achat.

En **figure 12**, on observe la mise en oeuvre de l'invention dans le cadre de la solution de paiement connue de l'homme du métier sous le nom de GlobeId (marque déposée) ou Kleline (marque déposée).

Ce système repose sur le principe de porte-monnaie virtuel (PMV). Il s'agit, en fait, d'un avoir que le client dépose au préalable et qui est débité au fur et à mesure de ses achats. Les transactions sont d'une totale transparence pour le client. C'est le seul cas où client et serveur commerçant n'ont aucune relation directe.

Pour utiliser le système GlobeId, il suffit de télécharger une interface (appelée « Klebox », marque déposée, chez Kleline) et d'ouvrir un compte en s'adressant à GlobeOnLine (marque déposée) ou Kleline. Un client peut ouvrir plusieurs porte-monnaies virtuels.

L'ouverture du porte-monnaie virtuel peut s'effectuer instantanément, en ligne. Dans ce cas, les coordonnées bancaires sont chiffrées (technologie RSA) et envoyées par l'intermédiaire du réseau Internet. Elles peuvent également être transmises par le téléphone, la télécopie ou le courrier postal. En réponse, le service utilisant cette solution attribue au client un numéro de porte-monnaie et un code confidentiel.

A l'ouverture du porte-monnaie virtuel, le client effectue deux opérations : il donne son numéro de carte bancaire et les autres informations nécessaires, puis verse, sur le porte-monnaie virtuel, un montant de son choix. Le client peut consulter l'état de son porte-monnaie virtuel et y déposer de nouvelles sommes d'argent à tout moment. Il lui est également permis de retirer tout ou partie de son avoir.

Le porte-monnaie virtuel est lié à une ou plusieurs cartes bancaires. Le client a la possibilité de personnaliser ses cartes bancaires, en leur donnant des noms, afin de ne pas les confondre. Des techniques de dédoublonnage assurent qu'à une carte correspond bien une seule personne.

La transaction type se déroule comme suit :

- le client navigue sur le serveur commerçant. Quand un produit l'intéresse, il clique dessus et se déclare prêt à l'acheter en envoyant un bon de commande au serveur commerçant ;

- celui-ci émet un ticket de caisse à destination du serveur GlobeId. Ce ticket de caisse comprend, d'une part, la nature et le montant de l'achat et, d'autre part, le numéro de porte-monnaie virtuel du commerçant. Le tout est signé à partir du code confidentiel de ce dernier. Ensuite, GlobeId vérifie ce ticket (le serveur commerçant est alors authentifié) et le fait apparaître sur l'écran de l'ordinateur du client ;

- le client signe électroniquement ce ticket avec son code secret et le retourne à GlobeId ;

- GlobeId authentifie alors le client avec sa clé publique et valide la transaction. Si le client a décidé de payer avec sa carte, la validation a lieu auprès du réseau bancaire avec, éventuellement, une demande d'autorisation au réseau cartes bancaires. Si le client utilise son porte-monnaie virtuel, celui-ci est aussitôt débité du montant de la transaction ;

- L'ordinateur du client émet enfin un bon de caisse vers le serveur commerçant (justificatif de la transaction) qui remet alors la marchandise.

Toutes les communications dans les transactions sont chiffrées à l'aide de clés asymétriques de 512 bits.

Les inconvénients de ce protocole sont que, pour le commerçant, il faut posséder un numéro de porte-monnaie virtuel et un code confidentiel.

En regard de la figure 12, on observe que, dans un mode particulier de réalisation de la présente invention, mis en oeuvre en combinaison avec la solution GlobeId :

1. l'ordinateur du client 1201 choisit un bien ou un service sur un site commerçant 1202 et valide son achat.

2. Le serveur commerçant demande alors un " ticket " (récépissé) à l'ordinateur du client (échange " *GRT1* " sur la figure 12).

3. L'ordinateur du client soumet, à son tour, cette demande au serveur d'intermédiation 1203 (échange " *GRT 2* ").

4. La phase d'authentification est alors mise en oeuvre (échange « *CAC/CAR* ») avec un code dynamique appelé « TID » (pour « Transcode Identificateur ») généré par le serveur d'intermédiation et envoyé par l'intermédiaire d'un réseau de télécommunication, sous le forme d'un message court SMS, adressé au téléphone mobile 1204 dont le numéro correspond à l'abonné identifié par

l'identificateur « *userId* » du client, stocké dans la base de données 1206 du serveur d'authentification 1205.

Selon une variante non représentée, on fait calculer et envoyer le code dynamique TID directement par l'opérateur de télécommunication. Dans ce cas, le serveur d'intermédiation transmet les informations nécessaires au calcul du code dynamique TID, à l'opérateur de télécommunication.

Selon une autre variante non représentée, le client reçoit, sous forme de message court SMS, le montant de la transaction, en clair, associé au code d'authentification de transaction afin qu'il vérifie l'intégrité du montant de son achat.

5. Le code d'authentification de transaction reçu par l'intermédiaire du mobile du client est saisi sur l'ordinateur utilisé par le client et les informations de la transaction sont ajoutés au code dynamique TID et sont envoyées au serveur d'intermédiation (" IS ") qui vérifie la validité du code dynamique TID et valide, avec le serveur d'authentification, le code d'authentification de transaction reçu de l'ordinateur du client.

6. Le serveur d'intermédiation délivre alors un récépissé (échange « *GPT 3* »") à l'ordinateur du client qui l'adresse ensuite au serveur commerçant (échange « *GPT 4* »).

Le protocole « SSL » (Secure Socket Level) est un protocole de communication sécurisé entre deux entités. Le lecteur pourra se référer à la version 3.0, des spécifications édictant ce protocole, version de Mars 1996. Cette version est incorporée ici par référence.

le protocole SSL est un protocole développé par NETSCAPE. La phase de négociation au départ permet l'authentification du serveur commerçant et, optionnellement, celle du client. Une fois cette phase terminée, les échanges sont cryptés avec la clé générée par l'ordinateur du client.

Ainsi, le protocole de sécurité SSL code les données, authentifie le serveur et assure l'intégrité des messages pour une connexion TCP/IP (« Transport Telecommunication Protocol / Internet Protocol) :

. notamment, le chiffrement des données (RC4),

. l'authentification du serveur commerçant pour le client (différentes méthodes de chiffrement asymétrique),

. l'intégrité des données (MD2, MD5),

. la non répudiabilité des échanges, et

. optionnellement, l'authentification du client pour le serveur.

Pratiquement, le protocole SSL procure une sécurité de type « poignée de main » pour débuter toute connexion TCP/IP. La poignée de main permet, à l'ordinateur du client et au serveur commerçant, de se mettre d'accord sur le niveau de sécurité à utiliser et de remplir les conditions d'authentification pour la connexion. Ensuite, l'unique rôle du protocole SSL consiste à coder et décoder le flux d'octets du protocole application en cours (par exemple « HTTP », acronyme de « HyperText Transfer Protocol » pour « protocole de transfert hypertexte »). Cela signifie que toutes les informations contenues dans les demandes et réponses HTTP sont entièrement codées, y compris l'URL (acronyme de universal resolution location) que l'ordinateur du client requiert, le contenu de tous les formulaires soumis (tels que les numéros de cartes de crédit), toute information relative à l'autorisation d'accès HTTP (noms d'utilisateur et mot de passe) et toutes les données retournées par le serveur à l'ordinateur du client.

Des certificats SSL peuvent être édités par une entité accréditée à la fois pour le client et le commerçant. De manière usuelle, le client ne possède pas de certificat.

On observe, en **figure 13**, dans un mode particulier de réalisation de la présente invention, en combinaison avec le schéma de paiement SSL, que :

- l'ordinateur du client 1301 initie d'abord l'achat, en choisissant son bien ou service sur le site commerçant 1302 ou la galerie commerçante souhaitée ;

- le déclenchement du paiement est activé par une validation d'achat du client (par exemple, l'appui sur une touche « validation achat ») ;

- s'ensuit l'ouverture de la communication SSL avec un échange, entre l'ordinateur du client 1301 et le serveur commerçant 1302, de trames qui permettent de régler les paramètres de la communication (version de protocole, numéro de session, algorithme de chiffrement retenu, méthode de compression, authentification réciproque et utilisation ou non de chiffrement à base d'algorithmes à clés publiques ou privées). Une clé maître est échangée, chiffrée, avec la clé privée du commerçant, l'ordinateur du client la déchiffrant avec la clé publique du commerçant et générant ensuite une clé de session basée sur cette clé maître. Cette opération

est reproduite sur le serveur commerçant afin de disposer, de part et d'autre, de la même clé de session. Ladite clé de session sert à chiffrer la communication entre l'ordinateur du client et le serveur commerçant ;

- le client tape un identificateur « *UserId* » permettant de l'identifier auprès du serveur commerçant ou de la galerie marchande ;

- le serveur commerçant ou de la galerie transmet l'identificateur « *UserId* » et les paramètres de la transaction, au logiciel de télépaiement 1303 qui calcule le code d'authentification de transaction et l'envoie, par l'intermédiaire d'un message court SMS, au client identifié par son numéro de téléphone mobile 1304 correspondant à son identificateur « *UserId* », dans la base des abonnés 1305 du serveur d'authentification 1306 ;

Une variante consiste à mettre en oeuvre le certificat SSL sur l'ordinateur du client, notamment en y incorporant, lors de sa génération par le serveur d'accréditation, le numéro de mobile utilisateur, le numéro de carte bancaire et la date limite de validité de la carte bancaire. Lors des échanges du début de connexion SSL, le serveur commerçant déchiffre les informations du certificat client et notamment le numéro de mobile qui sert à envoyer le code d'authentification de transaction client. Dans cette variante, il est ainsi possible de s'affranchir de la base de données abonnés dans le serveur d'authentification.

Une autre variante consiste à ce que le client envoie directement le numéro de carte bancaire et la date limite de validité de celle-ci. Dans ce cas, le serveur commerçant calcule un code d'authentification de transaction et récupère le numéro de mobile du client dans la base de données indexée par le numéro de carte bancaire. Ensuite, le code d'authentification de transaction est envoyé au client par l'intermédiaire de son mobile.

- le client identifié par son mobile reçoit le code d'authentification de transaction sur son téléphone mobile, puis le saisit dans un champ d'authentification sur l'écran de son PC ;

- le code d'authentification de transaction est envoyé par l'intermédiaire du serveur commerçant ou de la galerie, puis au serveur d'authentification qui valide alors le code d'authentification de transaction et déclenche le paiement.

- une variante consiste à joindre, en plus du montant de l'achat, les références du produit acheté, les quantités, ... , en clair, avec le code

d'authentification de transaction par l'envoi du message court SMS, lors de l'envoi sur le téléphone mobile du client.

Selon une variante (non représentée) de chacun des modes de réalisation de la présente invention, le serveur du commerçant effectue une opération de sélection des transmissions qui sont sécurisées conformément à la présente invention. Au cours de cette opération de sélection de transmissions, en fonction de critères prédéterminés, les transmissions sont classées en deux groupes, l'un concernant les transmission dites « à sécuriser » et l'autres les transmissions dites « normales ». Les transmissions « à sécuriser » sont traitées comme exposé ci-dessus, alors que les transmissions dites « normales » ne donnent pas lieu à plus d'une opération de transmission sur un support de communication. Les transmissions dites normales sont, en fait, conformes aux procédés connus dans l'art antérieur.

Par exemple, dans le cas du mode de réalisation exposé en figure 10, l'opération de sélection peut être faite au cours de l'opération 1005 ou au cours de l'opération 1008, en prenant, comme critère de sélection, le montant de transaction, et en le comparant à un montant limite de transaction. Les transmissions dites « à sécuriser » sont, alors, celles auxquelles sont associées des montants de transaction supérieurs audit montant limite.

Les différents modes de réalisation de la présente invention (authentification, certification de message et paiement électronique en ligne) peuvent être combinés afin de réaliser des applications spécifiques correspondant aux exigences de l'opérateur du service.

L'invention s'applique notamment :

- au contrôle d'accès sur site informatique (pour la sécurité interne à une entreprise, pour le télétravail dans une entreprise, pour l'accès à des bases de données protégées ...),

- à la remise d'information confidentielle en main propre (pour le courrier électronique, la télécopie sécurisée et/ou recommandée, pour la certification de devis ou de bon de commande ...),

- au paiement en ligne (pour le commerce électronique, pour la distribution d'information et ou de logiciels, ...),

- à la certification de message (pour la déclaration à distance, pour la banque à domicile, ...),

- à la remise de propositions commerciales personnalisées (pour les boîtes aux lettres sécurisées, ...),

- à la prise de pari, en ligne (pour les loteries ou les mises pour jeu de casinos, courses, ...),

- à la commande et à la réservation d'un programme de télévision (pour la télévision à facturation des seules émissions vues),

- à l'envoi d'information ou au téléchargement de logiciel à la demande,

- à la réservation de services en ligne ou

- à l'ouverture de porte-monnaie électronique virtuel.

Quelques unes de ces applications sont détaillées ci-dessous, à titre d'exemple.

Pour une **application de contrôle d'accès** mettant en oeuvre la présente invention, le réseau utilisé peut être un réseau connu sous le nom d'«intranet» ou un réseau mondial connu sous le nom d'«internet». L'objectif de cette application de l'invention est de s'assurer que l'utilisateur est une personne habilitée.

Dans cette application :

- l'utilisateur se met en relation avec le service,

- il s'identifie en fournissant un identifiant,

- il reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un mot de passe jetable,

- il tape ce mot de passe jetable sur le clavier de son terminal, puis

- si l'authentification est réalisée, il accède à la ressource considérée (pour la sécurité interne dans une entreprise, pour le télétravail ...).

Pour une **application de transmission de courrier électronique ou de télécopie recommandée** mettant en oeuvre la présente invention, le réseau utilisé peut être un réseau commuté. Les objectifs de cette application de l'invention sont :

- de s'assurer que la personne à qui est adressé le message sécurisé (le «destinataire»), le reçoit en main propre et

- de délivrer un certificat de message à l'émetteur et au destinataire du message sécurisé.

Dans cette application :

- l'utilisateur émetteur du message sécurisé compose le numéro d'un service spécialisé pour la mise en oeuvre de cette application,

- il s'identifie en fournissant un identifiant,

- il tape les coordonnées de l'utilisateur destinataire (numéro de téléphone, préférentiellement portable, adresse, télécopie, ...), puis

- il délivre son message sécurisé (oral, écrit et/ou par l'intermédiaire d'un télécopieur).

- il reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un certificat de message,

- il tape ce certificat de message sur le clavier de son terminal, sur le premier réseau,

- ce certificat de message est vérifié,

Ensuite, l'utilisateur destinataire :

- est informé qu'un message sécurisé l'attend (cette opération est réalisée par tout moyen connu (téléphonie, télécopie, courrier, pageur, courrier électronique ...),

- il compose le numéro du service spécialisé pour la mise en oeuvre de cette application,

- il s'identifie en fournissant un identifiant,

- il reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un certificat de message, et

- il tape ce certificat de message sur le clavier de son terminal, sur le premier réseau,

- ce certificat de message est vérifié,

- l'utilisateur destinataire du message sécurisé reçoit ce dernier,

- l'utilisateur émetteur est informé que le message sécurisé a été retiré par le destinataire.

Le service spécialisé conserve une trace de chacun des certificats ainsi délivrés.

Pour une **application à la télédéclaration** (c'est-à-dire de déclaration à distance) mettant en oeuvre la présente invention, le premier réseau utilisé peut être un réseau mondial connu sous le nom d'«internet». L'objectif de cette application de l'invention est de permettre une déclaration administrative officielle immédiate, de délivrer un récépissé à l'utilisateur et de s'assurer de l'identité du déposant.

Dans cette application :

- l'utilisateur émetteur de la déclaration se connecte à un service administratif adapté à cette application (voir ci-dessus),
- il s'identifie en fournissant un identifiant,
- il effectue ladite déclaration ou rempli un formulaire administratif,
- il reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un certificat de message, et
- il tape ce certificat de message sur le clavier de son terminal.

Pour une **application de l'invention à l'achat et/ou le paiement en ligne** mettant en oeuvre la présente invention, le réseau utilisé est le réseau mondial connu sous le nom d'«internet» et un logiciel mis en oeuvre par l'ordinateur de l'utilisateur permet de crypter un numéro de compte ou de carte bancaire (par exemple avec un logiciel de cryptage «SSL» ou « SET »). L'objectif de cette application de l'invention est de pouvoir payer en ligne en authentifiant la personne qui réalise la transaction.

Dans cette application :

- l'utilisateur se met en relation avec une «galerie marchande», c'est-à-dire un site rassemblant des commerçants fournissant des biens, des services ou de l'information,
- il s'identifie en fournissant un identifiant,
- il choisit une transaction qu'il souhaite effectuer,
- il indique un mode de paiement (carte bancaire, par exemple),
- il envoie au serveur de la galerie marchande son numéro de carte et la date de péremption de cette carte, sous protocole de cryptage SSL,
- le serveur génère un certificat de transaction auquel il associe le montant de transaction, en clair,

- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), ce certificat de transaction et le montant de la transaction en clair,
- il vérifie l'intégrité du montant,
- il tape ces éléments sur le clavier de son terminal, et
- la transaction est ensuite effectuée selon des procédures bancaires connues.

Pour une **application mettant en oeuvre la présente invention dans laquelle de l'information (textes, images, graphiques, sons) et/ou des logiciels sont fournis à la demande**, le réseau utilisé est le réseau mondial connu sous le nom d'«internet». L'objectif de cette application de l'invention est de faire payer à l'acte la personne qui accède à une ressource à valeur ajoutée et, de lui fournir le service demandé (transmission d'information ou de logiciel) en temps réel.

Dans cette application,

- l'utilisateur se met en relation avec le fournisseur de service,
- il s'identifie en fournissant un identifiant,
- il choisit une information ou un logiciel qui l'intéresse,
- le fournisseur de service indique le prix du service considéré,
- l'utilisateur confirme sa volonté d'achat,
- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un certificat de transaction assorti du montant de la transaction en clair, et
- il vérifie l'intégrité du paiement,
- il tape le certificat de transaction sur le clavier de son terminal,
- le certificat de transaction est vérifié,
- il reçoit l'information ou le logiciel considéré, et
- il est facturé par relevé mensuel par son opérateur de service de télécommunication, ou par son fournisseur d'accès au réseau, par exemple, en fonction de sa consommation.

Pour une **application de prise de paris à distance** mettant en oeuvre la présente invention, le réseau utilisé est le réseau mondial connu sous le nom d'«internet». L'objectif de cette application de l'invention est de s'assurer que la

personne misant sur un jeu ou prenant un pari à distance est habilitée à le faire et qu'elle a acquitté au préalable les droits nécessaires pour ce jeu.

Dans cette application :

- l'utilisateur ouvre et provisionne son compte chez l'opérateur de service, soit en déposant une somme sur son compte depuis un point de vente quelconque ou par chèque, soit en utilisant la même méthode que dans les applications de l'invention détaillée ci-dessus pour le paiement en ligne,
- puis, lorsque l'utilisateur veut participer à un jeu ou prendre un pari :
- il s'identifie en fournissant un identifiant, et/ou un numéro d'abonné,
- il sélectionne le jeu sur lequel il souhaite miser,
- l'utilisateur reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un certificat de transaction assorti de la mise et du pari, en clair, et
- il vérifie la mise et le pari
- il tape le certificat de transaction sur le clavier de son terminal,
- le certificat de transaction est vérifié (mise, pari, chiffres, combinaison).

Pour une **application à la fourniture d'offres personnalisées** mettant en oeuvre la présente invention, le réseau utilisé est le réseau mondial connu sous le nom d'«internet». L'objectif de cette application est d'identifier les demandes du consommateur en amont de l'acte d'achat et de lui faire des offres personnalisées correspondant à sa demande.

Dans cette application, lors de sa première connexion :

- le consommateur se met en relation avec le service,
- il s'identifie en fournissant un identifiant et/ou un numéro d'abonné,
- il reçoit, par l'intermédiaire d'un deuxième support de communication (par exemple téléphone portable ou pageur), un mot de passe jetable,
- il tape le mot de passe jetable sur le clavier de son terminal, et
- il remplit un questionnaire marketing permettant de définir les types de propositions commerciales à lui adresser.

Lorsqu'une proposition commerciale correspondant à sa demande lui est adressée, le consommateur reçoit un message «d'alerte», par l'intermédiaire du deuxième support de communication. Au cours de la deuxième connexion :

- le consommateur se met alors en relation avec le service,
- il s'identifie en fournissant un identifiant et/ou un numéro d'abonné,
- il reçoit, par l'intermédiaire d'un deuxième support de communication, un certificat de message,
- il tape le certificat de message sur le clavier de son terminal,
- il accède à la boîte aux lettres personnelle et confidentielle qui contient la proposition commerciale,
- il consulte la proposition.

REVENDICATIONS

1. Procédé de transmission d'information sur un premier support de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de communication,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur un terminal à adresse unique sur un deuxième support de communication, et

. une opération de transmission, sur le premier support de communication, d'un message confidentiel représentatif de ladite information confidentielle.

2. Procédé de transmission d'information sur un premier support de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un terminal à adresse unique sur ledit premier support de communication, d'une session de communication avec un moyen de communication situé à distance,

et, durant ladite session :

. une opération de réception d'une information confidentielle sur le premier support de communication, et

. une opération de transmission, sur un deuxième support de communication, d'un message confidentiel représentatif de ladite information confidentielle.

3. Procédé de transmission d'information sur un premier support de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture, par l'intermédiaire d'un premier terminal, d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de communication,

- une opération d'ouverture, par l'intermédiaire d'un deuxième terminal, d'une session de communication avec un moyen de communication situé à distance, sur un deuxième support de communication,

- lorsque les deux sessions sont ouvertes, une opération de réception d'une information confidentielle sur un desdits supports de communication sur lequel l'un des terminaux a une adresse unique, et

- une opération de transmission, sur l'autre desdits supports de communication, d'un message confidentiel représentatif de ladite information confidentielle.

4. Procédé de transmission d'information sur un premier support de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture d'une session de communication avec un moyen de communication situé à distance, sur ledit premier support de communication,

et, durant ladite session :

. une opération de génération d'une information confidentielle et de transmission de ladite information confidentielle, à un terminal à adresse unique sur un deuxième support,

. une opération de réception, sur le premier support de communication, d'un message confidentiel susceptible d'être représentatif de ladite information confidentielle, et

. une opération de vérification de correspondance entre ledit message confidentiel et ladite information confidentielle.

5. Procédé de transmission d'information sur un support de communication dit "deuxième", ledit support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative d'une durée de la première session.

6. Procédé de transmission d'information sur un support de communication dit "deuxième", ledit support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur prédéterminé.

7. Procédé de transmission d'information sur un support de communication dit "deuxième", ledit support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un terminal dit "deuxième", d'un premier message représentatif :

. d'un identifiant d'un terminal dit "troisième" possédant une adresse unique sur ledit réseau,

. d'une information confidentielle,

. d'une information représentative d'un montant de transaction,

- une opération de transmission, au troisième terminal, d'un deuxième message représentatif :

. de ladite information confidentielle et

. dudit montant,

- une opération de réception d'un troisième message, de la part dudit deuxième terminal, représentatif d'une validation de transaction, et

- une opération d'incrémentation d'un registre correspondant audit troisième terminal, d'une valeur représentative dudit montant de transaction.

8. Procédé de transmission d'information, entre un premier et un deuxième terminal, sur un premier support de communication appartenant à un réseau de communication, caractérisé en ce qu'il comporte :

- une opération d'ouverture de session de communication, sur le premier support de communication entre le premier et le deuxième terminal et

- une opération de transmission, de la part du deuxième terminal à un troisième terminal raccordé à un deuxième réseau et possédant une adresse unique sur ledit deuxième réseau, d'un premier message représentatif d'une information confidentielle,

- une opération de transmission, à une adresse sur ledit réseau qui correspond audit troisième terminal d'un deuxième message représentatif de ladite information confidentielle, et

- une opération de transmission, sur le premier support de communication, en provenance du premier terminal et à destination du deuxième terminal, d'un message représentatif de l'information confidentielle.

9. Procédé de transmission d'information sur un premier support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un premier terminal, d'un premier message représentatif :

. d'un montant d'une transaction envisagée,

. d'un identifiant d'un débiteur,

- une opération de transmission, sur un deuxième support de communication, à un serveur bancaire, d'un deuxième message représentatif :

. dudit montant,

. d'un identifiant dudit débiteur

. d'une demande d'autorisation de débit,

- une opération de réception ou non de la part dudit serveur bancaire, d'un troisième message représentatif d'une autorisation de débit,

- lorsque l'autorisation est accordée, une opération de transmission, à un deuxième terminal possédant une adresse unique sur un deuxième réseau de communication, d'un quatrième message représentatif d'une information confidentielle,

- une opération de réception, de la part dudit premier terminal, d'un cinquième message représentatif de ladite information confidentielle,

- une opération de vérification de correspondance entre le message confidentielle et l'information confidentielle.

10. Procédé de transmission d'information sur un premier support de communication faisant partie d'un réseau de communication, caractérisé en ce qu'il comporte :

- une opération de réception, de la part d'un premier terminal, d'un premier message représentatif :

. d'un montant d'une transaction envisagée,

. d'un identifiant d'un débiteur,

- une opération d'autorisation, ou non, de débit d'un compte bancaire,

- lorsque l'autorisation est accordée, une opération de transmission, à un deuxième terminal possédant une adresse unique sur un deuxième réseau de communication, d'un deuxième message représentatif de l'information confidentielle,

- une opération de réception, de la part dudit premier terminal, d'un troisième message représentatif de ladite information confidentielle,

- une opération de vérification de correspondance entre le message confidentielle et l'information confidentielle et

- dans le cas où la correspondance est vérifiée, une opération de débit dudit montant sur ledit compte bancaire.

11. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 10, caractérisé en ce que l'information confidentielle est représentative d'un numéro de session attribué à ladite session.

12. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 11, caractérisé en ce que l'information confidentielle est représentative d'un nombre pseudo-aléatoire.

13. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 12, caractérisé en ce que l'information confidentielle est représentative de l'heure et la date de ladite opération d'ouverture de session.

14. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 13, caractérisé en ce que l'information confidentielle est représentative d'un identifiant de l'utilisateur.

15. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 14, caractérisé en ce que l'information confidentielle est modifiée à chacune des sessions.

16. Procédé de transmission d'information selon l'une quelconque des revendications 1 à 15, caractérisé en ce que l'information confidentielle est représentative d'un ou plusieurs numéros de compte bancaire et/ou de carte de paiement.

17. Procédé de transmission selon l'une quelconque des revendications 1 à 16, caractérisé en ce que, au cours de l'opération de réception d'une information confidentielle, on reçoit, en outre, un montant de transaction.

18. Procédé de transmission selon l'une quelconque des revendications 1 à 17, caractérisé en ce que, au cours de l'opération de transmission d'un message confidentiel représentatif de l'information confidentielle, on transmet, en outre, un montant de transaction.

19. procédé de transmission selon la revendication 9, caractérisé en ce qu'après l'opération de vérification de correspondance, en cas de correspondance, il comporte une opération d'incrémentation d'un compte au débit dudit débiteur.

20. Procédé de transmission selon l'une quelconque des revendications 9 ou 19, caractérisé en ce qu'il comporte, après l'opération de réception du premier message, une opération de lecture, dans une base de donnée, de l'adresse unique du deuxième terminal sur le deuxième réseau.

21. Procédé de transmission selon l'une quelconque des revendications 9, 19 ou 20, caractérisé en ce qu'il comporte, après l'opération de réception du premier message, une opération de lecture, dans une base de donnée, d'un identificateur dudit serveur bancaire.

22. Procédé de transmission selon l'une quelconque des revendications 1 à 21, caractérisé en ce qu'il comporte une opération de saisie manuelle, au cours de laquelle l'utilisateur saisit un message confidentiel représentatif de l'information confidentielle.

23. Procédé de transmission selon l'une quelconque des revendications 1 à 22, caractérisé en ce qu'il comporte une opération de sélection de transmission, au cours de laquelle, en fonction de critères prédéterminés, les transmissions sont classées en deux groupes, l'un concernant les transmission dites « à sécuriser » et l'autres les transmissions dites « normales », les transmissions normales ne donnant pas lieu à plus d'une opération de transmission sur un support de communication.

24. Procédé de transmission selon la revendication 23, caractérisé en ce que, au cours de ladite opération de sélection, on met en oeuvre un montant limite de transaction, les transmissions dites « à sécuriser » étant celles auxquelles sont associées les montants de transaction supérieurs audit montant limite.

25. Procédé de transmission selon l'une quelconque des revendications 1 à 24, caractérisé en ce qu'il comporte une opération de transmission d'une adresse unique sur l'un desdits réseaux.

26. Procédé de transmission selon la revendication 25, caractérisé en ce que, au cours de ladite opération de transmission d'une adresse unique, on transmet un certificat contenant une information représentative du ladite adresse unique.

27. Procédé de transmission selon la revendication 26, caractérisé en ce que ledit certificat répond à un protocole de sécurisation de paiement et comporte une information représentative de ladite adresse unique.

28. Serveur informatique, caractérisé en ce qu'il est adapté à mettre en oeuvre le procédé de transmission selon l'une quelconque des revendications 1 à 27.

29. Ordinateur, caractérisé en ce qu'il est adapté à mettre en oeuvre le procédé de transmission selon l'une quelconque des revendications 1 à 27.